Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate
CyberNotes

Issue #2003-17 *August 25, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between August 4 and August 21, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Alt-N Technol-ogies[1]	Windows 95/998/ME/ NT 4.0/2000, XP	Deerfield MDaemon 5.0.5	A vulnerability exists in the SMTP authentication feature because a null password may be entered, which could let a remote malicious user obtain unauthorized access.	No workaround or patch available at time of publishing.	MDaemon SMTP Server Null Password	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[1] Secunia Security Advisory, August 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
attila-php.net [2]	Windows, Unix	Attila PHP 3.0	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'Rubrique' parameter in 'index.php3' due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code; a script injection vulnerability exists in the 'Titre,' 'Texte,' and 'Texte associé au lien' fields in 'user_action.php3' due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code; and a path disclosure vulnerability exists when certain characters are supplied to parameters, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Atilla PHP Content Management System Multiple Web	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
auto respond[3]	Unix	auto respond 2.0.2	A buffer overflow vulnerability exists due to a boundary error when handling e-mails, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://security.debian.org/pool/updates/contrib/a/autorespond/au	Autorespond Remote Buffer Overflow CVE Name: CAN-2003-0654	**High**	Bug discussed in newsgroups and websites.
Brian Benzinger [4]	Windows, Unix	Poster 2.0	A vulnerability exists due to the application failing to lock the 'setup' variable after initialization, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	Poster Administrative Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Cerberus[5]	Multiple	FTP Server 1.71	A remote Denial of Service vulnerability exists when the order of a carriage return and line feed are prefixed to a specific command, rather then appended.	No workaround or patch available at time of publishing.	FTPServer Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Chaogic Systems [6]	Unix	vhost-3.05r3	A remote Denial of Service vulnerability exists when a malicious user submits a long request to the vpop3d POP3 server.	No workaround or patch available at time of publishing.	vHost POP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

[2] Security Corporation Security Advisory, SCSA-020, August 18, 2003.
[3] Debian Security Advisory, DSA 373-1, August 16, 2003.
[4] Secunia Security Advisory, August 18, 2003.
[5] Secunia Security Advisory, August 20, 2003.
[6] Secunia Security Advisory, August 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[7] ***Proof of Concept exploit published***[8]	**Multiple**	**IOS 8.2, 8.3, 9.0, 9.1, 9.14, R12.x, R11.x, 10.x, 11.x, 12.x**	**An information disclosure vulnerability exists in the echo service, which could let a remote malicious user obtain sensitive information.**	**Workaround:** **The vendor recommends disabling the udp-small-services using the following commands:** **no service udp-small-servers** **www.cisco.com/warp/public/707/cisco-sn-20030731-ios-udp-echo.shtml**	**IOS UDP Echo Service Information Disclosure**	**Medium**	**Bug discussed in newsgroups and websites.** ***Proof of Concept exploit script has been published.***
Cisco Systems[9]	Multiple	VoIP Phone CP-7910 3.0-3.2, CP-7940 3.0-3.2, CP-7960 3.0-3.2	A remote Denial of Service vulnerability exists when a malicious user submits a spoofed ARP message.	No workaround or patch available at time of publishing.	Cisco 7900 Series VoIP Phone Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[10]	Multiple	WebNS 5.0 0.038s	A remote Denial of Service vulnerability exists in the Online Diagnostics Monitor (ONDM) when a malicious user submits a flood of TCP SYN packets to the System Controller Module (SCM) on Cisco Content Service Switches.	Upgrade available at: http://www.cisco.com/en/US/products/hw/contnetw/ps789/prod_release_note09186a008014ee04.html	Content Service Switch ONDM Ping Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cisco Systems[11, 12]	Multiple	Cisco Works CD1 1st Edition-5th Edition, Common Manage-ment Foundation 2.0, 2.1, Resource Manager 1.0, 1.1, Resource Manager Essentials 2.0-2.2	Several vulnerabilities exist: a vulnerability exists in the default configuration because the guest account is enabled with a blank password, which could let a malicious user circumvent authentication to obtain unauthorized administrative access; and a vulnerability exists when a specially crafted URL is submitted, which could let a remote malicious user execute arbitrary code.	**Workaround:** Cisco recommends disabling the Guest account as a workaround for the authentication bypass vulnerability until patches are available.	CiscoWorks Common Management Foundation Administrative Authentication Bypass & Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[7] Cisco Security Notice, 44261, July 31, 2003.
[8] SecurityFocus, August 8, 2003.
[9] SecurityFocus, August 12, 2003.
[10] S 2 1 S E C Advisory, August 7, 2003.
[11] Portcullis Security Advisory, August 13, 2003.
[12] Cisco Security Advisory, 44502, August 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Cisco Systems[13]	Multiple	all IOS software versions except 12.3 and 12.3T	A buffer overflow vulnerability exists when a malformed HTTP GET request that contains two gigabytes of data is submitted, which could let a remote malicious user execute arbitrary code.	Workaround and patches available at: http://www.cisco.com/warp/public/707/cisco-sn-20030730-ios-2gb-get.shtml	IOS 2GB HTTP GET Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit scripts have been published.
Clickcess Ltd [14]	Windows	ChitChat. NET 2.0	A Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code from the 'Name' and 'Topic Title' fields, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	ChitChat.NET Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Computer Associates [15]	Windows NT	eTrust Antivirus EE 7.0	A vulnerability exists because access to system resources such as system accounts and system processes for authentication may be restricted when the Realtime Monitor detects a virus, causing the NT Local System account to be quarantined.	Patch available at: http://esupport.ca.com/premium/antivirus/downloads/nt/7.0/QO41975.asp	eTrust Antivirus EE System Account Lockout	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cool Com-ponents[16]	Multiple	Testbuddy	A vulnerability exists because usernames and passwords are stored in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Testbuddy Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cryptcat[17]	Multiple	Cryptcat 1.10	A vulnerability exists because connections are not encrypted when run in server mode (even when instructed to do so via the -e command line switch), which could result in a false sense of security and potentially expose sensitive information.	No workaround or patch available at time of publishing.	Cryptcat Encrypted Connection Weakness	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Dame Ware Develop-ment LLC[18]	Windows NT 4.0/2000, XP	Mini Remote Control Server 3.69 & prior	A vulnerability exists when a specially crafted Windows Message is sent to the higher privileged DWRCS.exe process, which could let a malicious user execute arbitrary code with SYSTEM privileges.	Upgrade available at: http://www.dameware.com/download/default.asp#dmrc	Mini Remote Control Server System Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

[13] Cisco Security Notice, 44226, August 4, 2003.
[14] Zone-h Security Team Advisory, ZH2003-24SA, August 13, 2003.
[15] NTBugtraq, August 18, 2003.
[16] SecurityFocus, August 8, 2003.
[17] SecurityFocus, August 16, 2003.
[18] SecurityTracker Alert ID, 1007498, August 14, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Daniel Stenberg[19]	Unix	curl 7.1, 7.1.1, 7.2, 7.2.1, 7.3, 7.4, 7.4.1, 7.10.1, 7.10.3-7.10.6	A vulnerability exists when proxy authentication is used in a 'CONNECT' request, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://curl.haxx.se/download.html	cURL Proxy Authentication Header Information Leakage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
DC Scripts[20]	Windows, Unix	DCForum+ 1.2	A Cross-Site Scripting vulnerability exists in the 'Subject' field due to insufficient sanitization of HTML code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	DCForum+ Subject Field Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
ddskk/ skk[21] ***RedHat issues advisory[22]***	**Unix**	**ddskk 11.6.rel.0; skk 10.62 a**	**A vulnerability exists when temporary files are created due to insufficient security precautions, which could let a malicious user obtain elevated privileges.**	**Upgrades available at: http://security.debian.org/pool/updates/main/d/ddskk/** **http://security.debian.org/pool/updates/main/s/skk/** ***RedHat:* ftp://updates.redhat.com/**	**SKK/DDSKK Insecure Temporary Files** **CVE Name: CAN-2003-0539**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
DeskSoft [23]	Windows	CheckMail 1.2	A password disclosure vulnerability exists because usernames and passwords for associated e-mail accounts are stored in the Windows registry, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	CheckMail Password Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Dream-cost LLC [24]	Windows, Unix	HostAdmin	A path disclosure vulnerability exists when invalid queries are conducted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	HostAdmin Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Dropbear [25]	Unix	SSH Server 0.28-0.34	A format string vulnerability exists in the default configuration when the 'syslog()' function is called during authentication, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://matt.ucc.asn.au/dropbear/	SSH Server Format String	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[19] SecurityFocus, August 16, 2003.
[20] Zone-h Security Team Advisory, ZH2003-21SA, August 10, 2003.
[21] Debian Security Advisory, DSA 343-1, July 8, 2003.
[22] Red Hat Security Advisory, RHSA-2003:241-01, August 11, 2003.
[23] SecurityTracker Alert ID, 1007517, August 18, 2003.
[24] Securiteam, August 13, 2003.
[25] 0xbadc0ded Advisory #02, August 17, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
DWebPro [26]	Multiple	DWebPro 3.4.1	A vulnerability exists in the 'http.ini' file because authentication credentials can be viewed in plaintext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	DWebPro 'Http.ini' Plaintext Password Storage	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ecartis Project [27]	Unix	Ecartis 1.0.0 snapshot 20030417, 20030416, 20030404, 20030318, 20030312, 20030309, 20030303. 20030227, 20021013, 20020427, 20020125, 20020121	Several vulnerabilities exist: multiple buffer overflow vulnerabilities exist in the 'smtp.c,' 'unhttp.c,' and 'unmime.c' files due to the way user-supplied input is handled, which could let a remote malicious user execute arbitrary code; and a vulnerability exists due to improper validation of user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ECartis Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Emule, Imule, xMule [28]	Unix	Emule 0.29a, 0.27c, 0.27b, 0.27, EMule+ 1.0, lmule 1.2.1, 1.3.1, xMule 1.4.2, 1.4.3, 1.5.4	Several vulnerabilities exist: a format string vulnerability exists in 'OP_SERVERMESSAGE' when a specially crafted message value is submitted to the connected target client, which could let a remote malicious user execute arbitrary code; a heap overflow vulnerability exists in the processing of the 'OP_SERVERIDENT' message, which could let a remote malicious user execute arbitrary code; a vulnerability exists because a server can be added to the network with a specially crafted server name containing format string characters, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists when a specially crafted sequence of packets is submitted, which could let a remote malicious user execute arbitrary code.	Update to eMule 0.30a available at: http://www.emule-project.net/index.php?s=downloads xMule version 1.4.3 (stable) has been released. However, it only fixes the Denial of Service and the packet sequence vulnerabilities. lmule is no longer supported.	eMule/Imule/ xMule Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[26] SecurityTracker Alert ID, 1007518, August 18, 2003.
[27] Securiteam, August 18, 2003.
[28] e-matters GmbH Security Advisory, August 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Eudora[29]	Windows NT 4.0/2000	WorldMail 2.0	A Cross-Site Scripting vulnerability exists in the search utility due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WorldMail Search Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
file[30, 31, 32] ***More updates issued***[33, 34, 35, 36] ***More updates issued***[37] ***Sun issues advisory***[38]	**Unix**	**file 3.28, 3.30, 3.32-3.37, 3.39, 3.40**	**A buffer overflow vulnerability exists in the file utility ELF parsing routines, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.**	**Upgrade available at:** ftp://ftp.gw.com/mirrors/pub/unix/file/file-3.41.tar.gz **RedHat:** **ftp://updates.redhat.com/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **OpenPKG:** **ftp://ftp.openpkg.org/** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-003.txt.asc** ***Debian:*** **http://security.debian.org/pool/updates/main/f/file/** ***Trustix:*** **http://www.trustix.net/pub/Trustix/updates/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse** ***Immunix:*** **http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/file-3.30-7_imnx_3.41_1.i386.rpm** ***Sun:*** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F56040**	**File ELF Routine Buffer Overflow** **CVE Name: CAN-2003-0102**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[29] Exploitlabs.com Advisory, EXPL-A-2003-020, August 12, 2003.
[30] OpenPKG Security Advisory, OpenPKG-SA-2003.017, March 4, 2 003.
[31] Mandrake Linux Security Update Advisory, MDKSA-2003:030, March 6, 2003.
[32] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:086-07, March 7, 2003.
[33] NetBSD Security Advisory, 2003-003, March 12, 2003.
[34] Debian Security Advisory, DSA-260-1, March 13, 2003.
[35] Trustix Secure Linux Bugfix Advisory, TSL-2003-0006, March 18, 2003.
[36] SuSE Security Announcement, SuSE-SA:2003:017, March 21, 2003.
[37] Immunix Secured OS Security Advisory, IMNX-2003-7+-012-01, June 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeBSD [39]	Unix	FreeBSD 4.0-4.8, 5.0, 5.1, 4.1.1 – STABLE-4.7 – STABLE, 4.1.1 – RELEASE-4.3 – RELEASE, 4.5 – RELEASE-4.7 – RELEASE, 4.3 – RELENG, 4.4 – RELENG	An information disclosure vulnerability exists due to the IBCS2 system call translator for "statfs()" erroneously using the user-supplied length parameter when copying kernel data structures, which could let a malicious user obtain sensitive information.	Patches available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:10/ibcs2.patch	FreeBSD IBCS2 System Call Translator Information Disclosure	Medium	Bug discussed in newsgroups and websites.
FreeBSD [40]	Unix	FreeBSD 4.2-4.8, 5.0, 5.1	A Denial of Service vulnerability exists in the ptrace() system call and the spigot device driver due to a insufficient sanity checks when handling signal numbers.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:09/signal47.patch	FreeBSD Ptrace/SPIgot Denial of Service	Low	Bug discussed in newsgroups and websites.
Fusionphp [41]	Windows, Unix	Fusion News 3.3	A vulnerability exists due to insufficient login verification, which could let a remote malicious user add accounts with administrative privileges.	No workaround or patch available at time of publishing.	Fusion News Unauthorized Administrative Access	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
geeeeksoft .com[42]	Windows, Unix	geeeek Shop 1.4	Multiple information disclosure vulnerabilities exist when invalid URI parameters are submitted to geeeekShop scripts, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Multiple geeeekShop Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Gerd Knorr[43]	Unix	xpcd 2.0 8	A buffer overflow vulnerability exists in 'xpcd-svga' when a specially crafted long value is supplied for the HOME environment variable, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: http://security.debian.org/pool/updates/main/x/xpcd/	XPCD Home Environment Variable Buffer Overflow CVE Name: CAN-2003-0649	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[38] Sun(sm) Alert Notification, 56040, August 5, 2003.
[39] FreeBSD Security Advisory, FreeBSD-SA-03:10.ibcs2, August 11, 2003.
[40] FreeBSD Security Advisory, FreeBSD-SA-03:09, August 11, 2003.
[41] Bugtraq, August 15, 2003.
[42] Zone-h Security Team Advisory, ZH2003-17SA, August 9, 2003.
[43] Debian Security Advisory, DSA 368-1, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [44]	Unix	HP-UX 11.0, 11.11	Reliability problems have been reported in some HP-UX systems when patches are applied, which could let a malicious user cause a Denial of Service.	Patches available at: ftp://ftp.itrc.hp.com/	HP Fixes Local Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Company [45]	Unix	Compaq Tru64 4.0 g PK3 (BL17), 4.0 f PK7 (BL18), 5.1 b PK2 (BL22), 5.1 a PK5 (BL23), 5.1 a PK4 (BL21), 5.1 PK6 (BL20)	A Denial of Service vulnerability exists through the EE device driver.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/	HP Tru64 EE Device Driver Denial of Service	Low	Bug discussed in newsgroups and websites.
HolaCMS Team [46]	Windows, Unix	HolaCMS 1.2.9 HolaCMS 1.2.10	A vulnerability exists in the 'htmltags.php' script due to a lack of authentication, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	HolaCMS 'htmltags.php' Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Horde Project [47]	Unix	Horde 1.2-1.2.8, 2.0-2.2.3	A vulnerability exists in the Application Framework because the session ID may be revealed as part of the URL, which could let a remote malicious user hijack a mail account.	Upgrade available at: http://ftp.horde.org/pub/horde/	Horde Application Framework Account Hijacking	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[44] SecurityFocus, August 14, 2003.
[45] SecurityFocus, August 13, 2003.
[46] Virginity Security Advisory 2003-001, August 13, 2003.
[47] PuCCiOLAB.ORG Security Advisories, PCL-0001, August 12, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
IBM[48]	Windows, Unix	Lotus Sametime 1.5, 3.0	Multiple vulnerabilities exist: a vulnerability exist because the secret key used for encryption/decryption is included directly in the login packet, which could let a remote malicious user obtain sensitive information; a vulnerability exists because encryption keys are included within instant messages and each encrypted message begins with 6 bytes of known plaintext, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because 10 byte RC2/40 keys are generated using only ASCII representations, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Sametime Multiple Encryption Implementation	Medium	Bug discussed in newsgroups and websites.
IBM[49] ***Exploit script has been published*** [50]	**Unix**	**DB2 Universal Database for AIX 6.0, 6.1, 7.0-7.2, Universal Database for HP-UX 6.0, 6.1, 7.0-7.2, Universal Database for Linux 6.0, 6.1, 7.0-7.2, Universal Database for Solaris 6.0, 6.1, 7.0-7.2**	**A vulnerability exists because members of group 'db2asgrp' can use the setuid root 'db2job' binary to write arbitrary files, which could let a malicious user obtain root privileges.**	**No workaround or patch available at time of publishing.**	**DB2 'db2job' Arbitrary File Overwrite**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit script has been published.***
Ideal Science, Inc. [51]	Windows	IdealBB 1.4.9 Beta	A Cross-Site Scripting vulnerability exists in the 'error.asp' script due to insufficient input validation, which could let a remote malicious user execute arbitrary code.	Patch available at: http://www.idealscience.com/site/support/default.aspx Membership is required in order to download this fix.	IdealBB Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[48] Bugtraq, August 6, 2003.
[49] Bugtraq, August 5, 2003.
[50] SecurityFocus, August 12, 2003.
[51] Zone-h Security Team, ZH2003-15SA, August 7, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
iMedia Software[52]	Unix	Store Builder	A path disclosure vulnerability exists if invalid queries are conducted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Better Basket Pro Store Builder Remote Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
iMedia Software[53]	Unix	Stellar Docs 1.2	Several vulnerabilities exist: an information disclosure vulnerability exists when a specially crafted malformed HTTP GET request is submitted, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because a default username and password may be used to obtain administrative access.	No workaround or patch available at time of publishing.	Stellar Docs Path Disclosure & Administrative Access	Medium/ **High** **(High if adminis-trative access can be obtained)**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
iMedia Software[54]	Unix	News Wizard 2.0	A path information vulnerability exists when an invalid request is submitted for a web resource, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	News Wizard Path Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Info-ZIP[55] ***Advisories issued[56, 57, 58]***	**Unix**	**UnZip 5.5**	**A Directory Traversal vulnerability exists during the handling of pathnames for archived files, which could let a remote malicious user obtain sensitive information.**	**Debian:** http://security.debian.org/pool/updates/main/u/unzip/ **Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/unzip-5.50-11_imnx_1.i386.rpm **OpenPKG:** http://pgp.openpkg.org/ **YellowDog:** ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/yellowdog-3.0/ ***Conectiva:*** **ftp://atualizacoes.conectiva.com.br/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com/**	**UnZip Directory Traversal** **CVE Name:**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**

[52] Zone-h Security Team Advisory, ZH2003-19SA, August 10, 2003.
[53] Zone-h Security Team Advisory, ZH2003-20SA, August 10, 2003.
[54] Zone-h Security Team Advisory, ZH2003-18SA, August 10, 2003
[55] Bugtraq, May 10, 2003.
[56] Red Hat Security Advisory, RHSA-2003:199-02, August 15, 2003.
[57] Conectiva Linux Security Announcement, CLA-2003:724, August 18, 2003.
[58] Mandrake Linux Security Update Advisory, MDKSA-2003:073-1, August 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Invision Power Services[59]	Windows, Unix	Invision Board 1.0, 1.0.1, 1.1.1, 1.1.2, 1.2	A Cross-Site Scripting vulnerability exists in the 'admin.php' script due to insufficient sanitization on user-supplied URI parameters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Invision Power Board Admin.PHP Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Jeremy Elson[60]	Unix	tcpflow 0.10-0.12, 0.20	A format string vulnerability exists in the 'print_debug_message()' function if IPNetMonitorX or IPNetSentryX utilities are installed, which could let a malicious user execute arbitrary code with root privileges.	Upgrade available at: ftp://ftp.circlemud.org/pub/jelson/tcpflow/tcpflow-0.21.tar.gz	TCPflow Format String CVE Name: CAN-2003-0671	**High**	Bug discussed in newsgroups and websites.
KDE[61] ***Upgrades now available*** [62, 63] ***RedHat issues another advisory***[64] ***Debian issues advisory***[65]	**Unix**	**Konqueror Embedded 0.1**	**A vulnerability exists because the Common Name (CN) field on X.509 certificates is not properly validated when a SSL/TLS session is negotiated, which could let a malicious server masquerade as a trusted server.**	***KDE:*** **ftp://ftp.kde.org/pub/kde/security_patches** ***RedHat:*** **ftp://updates.redhat.com/** ***Debian:*** **http://security.debian.org/pool/updates/main/k/kdelibs-crypto/**	**Konqueror Embedded Common Name Certificate Validation** **CVE Name: CAN-2003-0370**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Leon J Breedt[66]	Unix	pam-pgsql 0.5.1, 0.5.2	A format string vulnerability exists in pam-PGSQL when a specially crafted username is submitted, which could let a remote malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/p/pam-pgsql/	Pam-PGSQL Username Logging Remote Format String CVE Name: CAN-2003-0672	**High**	Bug discussed in newsgroups and websites.

[59] Bugtraq, August 9, 2003.
[60] @stake, Inc. Security Advisory, a080703-2, August 7, 2003.
[61] Bugtraq, May 7, 2003.
[62] KDE Security Advisory, June 2, 2003.
[63] Red Hat Security Advisory, RHSA-2003:192-01, June 5, 2003.
[64] Red Hat Security Advisory, RHSA-2003:193-08, June 17, 2003.
[65] Debian Security , DSA 361-2, August 9, 2003.
[66] Debian Security Advisory, DSA 370-1, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macro-media[67]	Windows, MacOS, Unix	ColdFusion Server MX 6.0, Developer's Resource Kit (DRK) vol. 4, vol. 2, Dream-weaver MX 6.0, 6.1, Dream-weaver Ultradev 4.0	Multiple Cross-Site Scripting vulnerabilities exist because the PHP User Authentication extensions (available in the DevNet Resource Kit) contain an input validation flaw in the "Log In User" function in the "Access Denied" variable, which could let a remote malicious user execute arbitrary code.	Patch information available at: http://www.macromedia.com/devnet/security/security_zone/mpsb03-05.html	Dreamweaver MX/DRK/ UltraDev Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Mark H. Weaver[68]	Unix	Netris 0.3-0.5	A buffer overflow vulnerability exists due to insufficient bounds checking when a server greeting is copied into an internal memory buffer, which could let a remote malicious user execute arbitrary code.	Patch available at: ftp://ftp.netris.org/pub/netris/netris-0.52.tar.gz ftp://ftp.netris.org/pub/netris/netris-0.5-0.52.diff **Debian:** http://security.debian.org/pool/updates/main/n/netris/	Netris Client-Side Buffer Overflow CVE Name: CAN-2003-0685	**High**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published. netric-client.
Martin Pool[69]	Unix	distcc 2.7, 2.9	A vulnerability exists in the 'distcc' distributed compiler due to the way temporary files are handled, which could let a malicious user obtain elevated privileges.	Upgrade available at: http://distcc.samba.org/ftp/distcc/distcc-2.10.tar.bz2	DistCC Elevated Privileges	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Matrikz GB[70]	Windows, Unix	Guestbook 2.0	Several vulnerabilities exist: a vulnerability exists in the 'index.php' edit function because an authenticated user can modify his/her profile and become an 'admin' user; and an authentication vulnerability exists because all usernames and passwords are stored in plain text, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	Guestbook Administrative Privilege Escalation	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser however an exploit has been published.
Metamail [71]	Unix	Metamail 2.7	Multiple vulnerabilities exist that could result in file corruption, execution of shell commands, or execution of arbitrary code.	**SCO:** ftp://ftp.caldera.com/pub/updates/UnixWare/CSSA-2003-SCO.15	Metamail Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.

[67] Macromedia Security Advisory, MPSB03-05, August 19, 2003.
[68] Debian Security Advisory, DSA 372-1, August 16, 2003.
[69] SecurityTracker Alert ID, 1007488, August 13, 2003.
[70] Bugtraq, August 16, 2003.
[71] SCO Security Advisory, CSSA-2003-SCO.15, August 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Meteor Soft[72]	Windows 98/SE	Meteor FTP 1.2, 1.5	A remote Denial of Service vulnerability exists when a malicious user submits a 'USER' command followed by large amounts of data. This could possibly be exploited to execute arbitrary code.	No workaround or patch available at time of publishing.	Meteor FTP Server USER Remote Denial of Service	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft [73]	Windows 2000	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Profes-sional, SP1-SP4, 2000 Server, SP1-SP4,	A vulnerability exists in the resource reservation protocol (RSVP) server, which could let a malicious user hijack management of the network.	No workaround or patch available at time of publishing.	Windows 2000 RSVP Server Authority Hijacking	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Microsoft [74] ***Microsoft updates bulletin*** [75]	**Windows 98/ME/NT 4.0/2000, XP, 2003**	**DirectX 5.2, 6.1, 7.0a, 7.0, 8.1, 9.0 a**	**Two buffer overflow vulnerabilities exists in the function used by DirectShow to check parameters in a Musical Instrument Digital Interface (MIDI) file, which could let a malicious user execute arbitrary code.** ***Bulletin updated to include details of an additional patch for versions of DirectX. and added clarification regarding additional patch in Technical description section.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-030.asp**	**DirectShow MIDI Filetype Buffer Overflows** **CVE Name: CAN-2003-0346**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Microsoft [76]	Windows 2000, XP	MDAC 2.5, RTM, SP1&SP2, 2.6, RTM, SP1&SP2, 2.7, RTM Refresh	A buffer overflow vulnerability exists in Microsoft Data Access components when a client or a SQL Server implementing the SQL-DMO library, sends a broadcast request for Microsoft SQL servers on a network, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-033.asp	Microsoft MDAC Buffer Overflow CVE Name: CAN-2003-0353	**High**	Bug discussed in newsgroups and websites.

[72] Securiteam, August 10, 2003.
[73] Bugtraq, August 11, 2003.
[74] Microsoft Security Bulletin, MS03-030, July 23, 2003.
[75] Microsoft Security Bulletin, MS03-030, V2.0 &2.1, August 20, 2003.
[76] Microsoft Security Bulletin, MS03-033, August 20, 2003

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [77] *Microsoft updates bulletin* [78]	Windows 98/NT 4.0/2000, XP	MDAC 1.5, 2.0, 2.1 Upgrade, 2.1 Clean, 2.1 2.4202.3 (GA) clean, 2.1 2.4202.3 (GA), 2.1.1 .3711.11 (GA), 2.5, 2.5 SP1&2, 2.5 RTM, 2.6, 2.6 SP1&2, 2.6 RTM, 2.7, 2.7 RTM Refresh	A buffer overflow vulnerability exists in the T-SQL OpenRowSet command, which could let a malicious user obtain complete control over the database, and potentially obtain administrative privileges. *Note: This issue is only exploitable if SQL Server is installed on a vulnerable system.* *Subsequent to the release of this bulletin, it was determined that the vulnerability addressed is not with the OpenRowSet command (which is a Microsoft SQL Server command) but rather that the vulnerability is with the underlying MDAC component Open Database Connectivity (ODBC), which is present in all versions of Windows. Additionally, the original patch released with this did not install correctly on some systems because of a flaw in the way that Microsoft Windows Installer updated the System File Protection cache. The bulletin has been updated to include this additional information and to direct users to an updated patch.* *Note: The patch for this security bulletin has been superceded by the patch in MS03-033. Customers who are seeking the patch for MS02-040 should instead install the patch for MS03-033.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-040.asp	Microsoft Data Access Components T-SQL Buffer Overflow CVE Name: CVE-CAN-2002-0695	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[77] Microsoft Security Bulletin, MS02-040, July 31, 2002.
[78] Microsoft Security Bulletin, MS02-040, V2.0, August 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [79]	Windows 95/98/ME/ NT 4.0/2000, 2003	Internet Explorer 5.01, SP1-SP3, 5.5, SP1-SP2, 6.0, SP1, 6.0 for Windows Server 2003	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'BR549.dl'l ActiveX control due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code; a Cross-Domain vulnerability exists in the way Internet Explorer retrieves files from the cache, which could let a remote malicious user execute arbitrary scripting in the "My Computer Zone;" and a vulnerability exists because Internet Explorer does not properly determine object types, which could let a remote malicious user execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-032.asp	Internet Explorer Multiple Vulnerabilities CVE Names: CAN-2003-0530, CAN-2003-0531, CAN-2003-0532	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published for the IE Object Type vulnerability.
Microsoft [80] ***Microsoft updates bulletin*** [81] ***Microsoft updates bulletin*** [82]	**Windows NT**	**Windows NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6**	**A remote Denial of Service vulnerability exists in the 'GetCanonicalPath()' function because memory that the function does not own can be freed when a specially crafted request is submitted, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.** ***Bulletin was updated to provide details of problem when patch is installed on systems running RRAS Service.*** ***Bulletin was updated to reflect the release of updated patches to correct problems on computers running RAS.***	**Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-029.asp**	**Windows NT File Management Function Remote Denial of Service** **CVE Name: CAN-2003-0525**	**Low**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Microsoft [83]	Windows NT 4.0	Visual Studio 6.0	A buffer overflow vulnerability exists in the activeX plugin, 'MCWNDX.OCX' due to improper verification of the 'Filename' property, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft MCIWNDX. OCX Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[79] Microsoft Security Bulletin, MS03-032, August 20, 2003.
[80] Microsoft Security Bulletin, MS03-029, July 23, 2003.
[81] Microsoft Security Bulletin, MS03-029 V1.1, July 29, 2003.
[82] Microsoft Security Bulletin, MS03-029 V2.0, August 13, 2003.
[83] SecurityTracker Alert ID, 1007493, August 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [84, 85] *Multiple exploits have been published and several Trojans circulating.*[86] *Mblast worm circulating in the wild.* *Microsoft updates bulletin*[87]	Windows 98/NT 4.0/2000, 2003, XP	Windows 2000 Advanced Server, SP1-SP4, 2000 Datacenter Server, SP1-SP4, 2000 Professional, SP1-SP4, 2000 Server, SP1-SP4, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Server 2003 Datacenter Edition, 64-bit, 2003 Enterprise Edition, 64-bit, Server 2003 Standard Edition, Server 2003 Web Edition, Windows XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists in the RPC interface that implements the Distributed Component Object Model services (DCOM) due to insufficient bounds checking of client DCOM object activation requests, which could let a malicious user install programs, view, change or delete data, create new accounts with full privileges or execute arbitrary code. *V1.4 Bulletin has been updated to include information about Windows 2000 Service Pack 2 support for this patch and updated bulletin with additional workaround information.* *V1.5 Added details for scanner tool.* *V1.6 Updated download links, removed the word "Server" from the NT4 link.* *V1.7 Corrected minor formatting errors in the Frequently Asked Questions section.* *V1.8 Updated supercedence information in the Additional Information section.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp	Windows DCOM RPC Buffer Overflow CVE Name: CAN-2003-0352	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media. *Multiple exploit scripts have been published. There is currently at least one autorooter-enabled IRC bot circulating that exploits this vulnerability. Also multiple Trojans are circulating that exploit the vulnerability.* *Another exploit script has been published.*

[84] Microsoft Security Bulletin, MS03-026 V1.2, July 21, 2003.
[85] Department of Homeland Security Advisory, July 24, 2003.
[86] SecurityFocus, August 8, 2003.
[87] Microsoft Security Bulletin, MS03-026 V1.4-V1.8, August 12, 14, 15, 18, & 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mini HTTP Server[88]	Windows 2000, XP	WebForum Server 1.5	A vulnerability exists because the administrative user account is created by default during installation and is assigned a blank password, which could let a remote malicious user obtain administrative access.	No workaround or patch available at time of publishing.	MiniHTTP Server WebForums Server Null Default Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[89]	Unix	FreeBSD FreeBSD 2.2-2.2.6, 2.2.8, 3.0-3.5.1, 4.0-4.8, 5.0, 5.1; Linux kernel 2.0-2.0.39, 2.2-2.2.25, 2.4-2.4.21; NetBSD NetBSD 1.0-1.2.1, 1.3-1.3.3, 1.4-1.4.3, 1.5-1.5.3, 1.6, 1.6.1; OpenBSD OpenBSD 2.0-2.9, 3.0-3.3	A vulnerability exists in the entropy pool implemented by the /dev/random device on various Unix-derived operating systems when the pool has been emptied, and the entropy mechanism begins to the seed the pool with a source of pseudo-random data, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Unix/Linux Keystroke Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[90, 91, 92, 93, 94, 95]	Unix	Conectiva Linux 7.0, 8.0; Wietse Venema Postfix 20011115, 20010228, 19990906, 1.0.21, 1.1.11, 1.1.12	A remote Denial of Service vulnerability exists in the address parser code when a malicious user creates a malformed envelope address.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Engarde:** http://www.linuxsecurity.com/advisories/engarde_advisory-3517.html **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Wietse Venema:** http://www.postfix.org/download.html	Postfix Malformed E-mail Envelope Address Remote Denial of Service CVE Name: CAN-2003-0540	Low	Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.

[88] SecurityFocus, August 7, 2003.
[89] Securiteam, August 18, 2003.
[90] Conectiva Linux Security Announcement, CLA-2003:717, August 4, 2003.
[91] Guardian Digital Security Advisory, ESA-20030804-019, August 4, 2003.
[92] Mandrake Linux Security Update Advisory, MDKSA-2003:081, August 4, 2003.
[93] Red Hat Security Advisory, RHSA-2003:251-01, August 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[96]	Windows NT 4.0/2000	Microsoft URLScan 2.5; RSA Security SecurID 5.0	An information disclosure vulnerability exists in RSA's SecurID when used with Microsoft URLScan due to the order in which the products are placed within the global ISAPI filter list, which could let a remote malicious user obtain sensitive information.	**Workaround:** RSA Security has suggested that until an official fix is available, users are advised to adjust the order of the global ISAPI filter list, to have the SecurID filter above the URLScan filter	Microsoft URLScan / RSA Security SecurID Configuration Enumeration	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors [97, 98, 99, 100]	Unix	CGI.pm 2.73-2.79, 2.93, 2.751, 2.753; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Mandrake Soft Corporate Server 2.1, 8.2, ppc, 9.0, 9.1, ppc, Single Network Firewall 7.2; OpenPKG Current, 1.2, 1.3	A Cross-Site Scripting vulnerability exists in the 'start_form()' function (or other functions that use this function) due to insufficient sanitization of user-supplied HTML and script, which could let a remote malicious user execute arbitrary code.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/p/perl/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** http://pgp.openpkg.org	Multiple Vendor CGI.pm 'Start_Form' Cross-Site Scripting CVE Name: CAN-2003-0615	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[94] SuSE Security Announcement, SuSE-SA:2003:033, August 4, 2003.
[95] Trustix Secure Linux Security Advisory, TSLSA-2003-0029, August 7, 2003.
[96] IRM Security Advisory No. 006, August 13, 2003.
[97] Conectiva Linux Security Announcement, CLA-2003:713, July 29, 2003.
[98] OpenPKG Security Advisory, OpenPKG-SA-2003.036, August 6, 2003.
[99] Debian Security Advisory, DSA 371-1, August 12, 2003.
[100] Mandrake Linux Security Update Advisory, MDKSA-2003:084, August 20, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [101] *Exploit script published and more upgrades issued* [102, 103, 104] *More advisories issued* [105, 106, 107]	Unix	Linux kernel 2.4.0-test1-2.4.0-test12, 2.4-2.4.17, 2.4.18, 2.4.18 x86, 2.4.18 pre-1-2.4.18 pre-8, 2.4.19, 2.4.19 - pre1-2.4.19 – pre6, 2.4.20, 2.4.21, 2.4.21 pre1, 2.4.21 pre4	Multiple vulnerabilities exist: an information disclosure vulnerability exists due to a flaw in '/proc/tty/driver/serial,' which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists due to a race condition in the execve() system call; an access control vulnerability exists because a malicious user can bind services to UDP ports that have already been allocated; an access control vulnerability exists in the 'execve()' because the file descriptor of an executable process is recorded in the calling process's file table, which could let a malicious user obtain sensitive information; a vulnerability exists in the '/proc' filesystem, which could let a malicious user obtain sensitive information; a remote Denial of Service vulnerability exists in the Spanning Tree Protocol (STP) implementation due to insufficient validation of user-supplied input; a vulnerability exists because the bridge topology can be modified due to the inherent insecurity of the STP protocol, which could let a remote malicious user modify information; and a vulnerability exists in the forwarding table, which could let a remote malicious user spoof packets.	Engarde: http://infocenter.guardiandigital.com/advisories/ RedHat: ftp://updates.redhat.com/ *Conectiva:* ftp://ul.conectiva.com.br/updates/ *Debian:* http://security.debian.org/pool/updates/main/k/ *Mandrake:* http://www.mandrakesecure.net/en/advisories/ *SuSE:* http://www.suse.de/de/private/download/updates/index.html *Debian:* http://security.debian.org/pool/updates/main/k/ *RedHat:* ftp://updates.redhat.com/	Multiple Linux 2.4 Kernel Vulnerabilities CVE Names: CAN-2003-0461, CAN-2003-0462, CAN-2003-0464, CAN-2003-0476, CAN-2003-0501, CAN-2003-0550, CAN-2003-0551, CAN-2003-0552	Low/ Medium (Medium if sensitive information can be obtained or elevated privileges are obtained)	Bug discussed in newsgroups and websites. *Proof of Concept exploit has been published for the execve() system call Denial of Service.*

[101] Red Hat Security Advisory, RHSA-2003:238-01, July 21, 2003.
[102] Mandrake Linux Security Update Advisory, MDKSA-2003:074, July 15, 2003.
[103] Conectiva Linux Announcement, CLSA-2003:712, July 28, 2003.
[104] Debian Security Advisories, DSA 358-21 & DSA 358-2, July 31, 2003 & August 5, 2003.
[105] SuSE Security Announcement, SuSE-SA:2003:034, August 12, 2003.
[106] Debian Security Advisory, DSA 358-4, August 13, 2003.
[107] RedHat Security Advisories, RHSA-2003:198-16 & 239-13, August 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [108, 109, 110]	Windows, OpenVMS, Unix	Compaq OpenVMS 7.1 Alpha, 7.1 -2 Alpha, 7.1 VAX, 7.2 -2 Alpha, 7.2 -1H2 Alpha, 7.2 -1H1 Alpha, 7.2 VAX, 7.2 Alpha, 7.2.1 Alpha, 7.3 VAX, Alpha, Tru64 5.0 a, 5.1 a, 5.1; Cray UNICOS 6.0 E, 6.0, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2.4 , 9.2, UNICOS MAX 1.3.5, 1.3, UNICOS/ mk 1.5, 1.5.1, 2.0.5.54; Entegrity DCE/DFS for Linux 2.1, DCE/DFS for Tru64 Unix 4.1.6, 4.2.2, PC-DCE for Windows 4.0.8, 5.0.1; HP HP-UX 10.20, 11.0; IBM DCE 2.2 for Windows, 3.1 for Solaris, AIX, 3.2 for Solaris, AIX	A remote Denial of Service vulnerability exists in multiple vendor OSF DCE (Distributed Computer Environment) implementations.	**Entegrity:** http://support.entegrity.com/private/patches/dce/rpcattacks.shtml **Hewlett Packard:** http://itrc.hp.com Patch PHSS_19739, Patch PHSS_17810 **IBM:** ftp://ftp.software.ibm.com/software/network/dce/support/ifixes/	Multiple Vendor OSF Distributed Computing Environment Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[108] CERT/CC Vulnerability Note, VU#377804, August 8, 2003.
[109] Hewlett-Packard Company Security Bulletin, HPSBUX0308-273, August 13, 2003.
[110] Hewlett-Packard Company Software Security Response Team, SSRT3608, August 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [111, 112, 113, 114, 115, 116, 117, 118] *More advisories issued* [119, 120, 121]	MasOS X, Unix	FreeBSD 4.0, alpha, 4.0.x, 4.1, 4.1.1, Stable, Release, 4.2, Release, Stable, Stablepre050201, pre122300, 4.3, Release, Releng, Stable, 4.4, Releng, Stable, 4.5, Release, Stable, 4.5 Stablepre2002-03-07, 4.6, Release, Stable, 4.6.2, 4.7, Release, Stable, 4.8, PreRelease 5.0, alpha; NetBSD 1.5-1.5.3, 1.6, 1.6.1; OpenBSD 2.0-2.9, 3.0-3.3; RedHat wu-ftpd-2.6.1-16.i386.rpm, 16.ppc.rpm, 18.i386.rpm, 18.ia64.rpm, -2.6.2-5.i386.rpm, 8.i386.rpm Washington University wu-ftpd 2.5.0, 2.6.0-2.6.3	A buffer overflow vulnerability exists due to an off-by-one error in the 'fb_realpath()' function when calculating the length of a concatenated string, which could let a remote malicious user obtain root privileges.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Debian:** http://security.debian.org/pool/updates/main/w/wu-ftpd/ **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:08/realpath.patch **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **NetBSD:** ftp://ftp.netbsd.org/pub/NetBSD/security/patches/SA2003-011-realpath.patch **OpenBSD:** ftp://ftp.OpenBSD.org/pub/OpenBSD/patches/ **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse *Apple:* http://docs.info.apple.com/article.html?artnum=61798 *Immunix:* http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/wu-ftpd-2.6.1-6_imnx_8.i386.rpm *Sun:* http://sunsolve.sun.com/patches/linux/security.html	Multiple Vendor realpath() Off-By-One Buffer Overflow CVE Name: CAN-2003-0466	High	Bug discussed in newsgroups and websites. Exploit scripts have been published. *Another exploit script has been published.*

[111] Debian Security Advisory, 357-1, July 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [122, 123, 124, 125] ***More patches released*** [126] ***Conectiva issues advisory*** [127]	**Unix**	**Mandrake Soft Corporate Server 2.1, Linux Mandrake 8.2, ppc, 9.0;** **Terra Soft Solutions Yellow Dog Linux 2.3, 3.0;** **ypserv ypserv 1.3.11, 1.3.12, 2.2, 2.5-2.7**	**A Denial of Service vulnerability exists in the Network Information Service (NIS) server when a malicious user queries ypserv via TCP and subsequently ignores the server's response.**	**Ypserv:** **ftp://ftp.kernel.org/pub/linux/utils/net/NIS/ypserv-2.8.tar.gz** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **RedHat:** **ftp://updates.redhat.com/** **Sun:** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55600** **YellowDog:** **ftp://ftp.yellowdoglinux.com/pub/yellowdog/updates/** ***Sun:*** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F55600** ***Conectiva:*** **ftp://ul.conectiva.com.br/updates/1.0/**	**Multiple Vendor YPSERV Denial of Service** **CVE Name: CAN-2003-0251**	**Low**	**Bug discussed in newsgroups and websites.**

[112] Mandrake Linux Security Update Advisory, MDKSA-2003:080,July 31, 2003.
[113] Red Hat Security Advisory, RHSA-2003:245-01, July 31, 2003.
[114] SuSE Security Announcement, SuSE-SA:2003:032, July 31, 2003.
[115] Conectiva Linux Security Announcement, CLA-2003:715, August 1, 2003.
[116] FreeBSD Security Advisory, FreeBSD-SA-03:08, August 4, 2003.
[117] NetBSD Security Advisory 2003-01, August 4, 2003.
[118] Turbolinux Security Advisory, TLSA-2003-46, August 4, 2003.
[119] Immunix Secured OS Security Advisory, IMNX-2003-7+-019-01, August 7, 2003.
[120] Apple Security Update, 61798, August 14, 2003.
[121] Sun Advisory, August 18, 2003.
[122] Red Hat Security Advisory RHSA-2003:173-01, June 25, 2003.
[123] Mandrake Linux Security Update Advisory, MDKSA-2003:072, June 27, 2003.
[124] Yellow Dog Linux Security Announcement, YDU-20030627-1, June 27, 2003.
[125] Sun(sm) Alert Notification, 55600, July 2, 2003.
[126] Sun(sm) Alert Notification, 55600, July 25, 2003.
[127] Conectiva Linux Announcement, CLSA-2003:722, August 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [128, 129, 130, 131, 132, 133]	Unix	Conectiva Linux 7.0, 8.0; Wietse Venema Postfix 20011115, 20010228, 19990906, 1.0.21, 1.1.11	A vulnerability exists because Postfix can allow a remote malicious user to 'bounce-scan' a private network. It can also be exploited to use the server as a Distributed Denial of Service tool.	**Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Engarde:** http://www.linuxsecurity.com/advisories/engarde_advisory-3517.html **Mandrake:** http://www.mandrakesecure.net/en/advisories/ **RedHat:** ftp://updates.redhat.com/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Wietse Venema:** http://www.postfix.org/download.html	Postfix Connection Proxying CVE Name: CAN-2003-0468	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Multipoint [134]	Windows	FTP-Server 0.2.3b	A Directory Traversal vulnerability exists due to missing validation of input to the 'GET' and 'LIST' commands, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.multipointftp.de/index.html	FTP-Server Directory Traversal	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
NetSurf[135]	Windows	NetSurf 3.02	A buffer overflow vulnerability exists in the URL handling due to insufficient bounds checking, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.klodware.narod.ru/	NetSurf Long URI Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[128] Conectiva Linux Security Announcement, CLA-2003:717, August 4, 2003.
[129] Guardian Digital Security Advisory, ESA-20030804-019, August 4, 2003.
[130] Mandrake Linux Security Update Advisory, MDKSA-2003:081, August 4, 2003.
[131] Red Hat Security Advisory, RHSA-2003:251-01, August 4, 2003.
[132] SuSE Security Announcement, SuSE-SA:2003:033, August 4, 2003.
[133] Trustix Secure Linux Security Advisory, TSLSA-2003-0029, August 7, 2003.
[134] Secunia Security Advisory, August 20, 2003.
[135] Securiteam, August 13, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetWin[136]	Windows NT 4.0/2000, XP, 2003, Unix	Surge LDAP 10.0d	Multiple vulnerabilities exist: a path disclosure vulnerability exists in the web server component when a HTTP GET request is issued for an invalid resource, which could let a remote malicious user obtain sensitive information; a remote Denial of Service vulnerability exists when a long URL is requested; a vulnerability exists in 'surgeldap\user.dat' because usernames and passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information; and a Cross-Site Scripting vulnerability exists in the 'user.cgi' script due to insufficient verification of the 'cmd' parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SurgeLDAP Multiple Vulnerabilities	Low/ Medium/ **High** **(Low if a DoS; Medium is sensitive informa-tion can be obtained; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required however, an exploit has been published. Denial of Service vulnerability may be exploited via a web browser.
Novell[137]	Multiple	iChain Server 2.2, FP1a, FP1	A vulnerability exists when a new user's session is opened on the same port as another user's session, which could let a malicious user inherit another user's session.	Upgrade available at: http://support.novell.com/servlet/filedownload/sec/ftf/ic22fp2.exe	iChain Session Inheritance	Medium	Bug discussed in newsgroups and websites.
Novell[138]	Multiple	Netware 5.1 SP6, 6.0 SP3, 6.5	Novell has released a new version of 'NWFTPD.NLM' for NetWare that provides security enhancements, bugfixes, and addresses a number of unspecified security issues, including two weaknesses involving anonymous FTP access. A loophole in intruder detection methods was also reported.	Upgrade available at: http://support.novell.com/servlet/filedownload/sec/ftf/nwftpd9.exe	NetWare NWFTPD. NLM Unspecified Security Vulnerabilities	Medium	Bug discussed in newsgroups and websites.
Novell[139]	Multiple	Netware 6.5	A remote Denial of Service vulnerability exists due to an error in 'XNFS.NLM' when being portscanned.	Upgrade available at: http://support.novell.com/servlet/filedownload/sec/ftf/xnfs1.exe	NetWare XNFS Portscan Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with Nessus and possibly other publicly available portscanning tools.

[136] Securiteam, August 14, 2003.
[137] Novell Technical Information Document, TID2966683, August 8, 2003.
[138] Novell Technical Information Document, TID2966658, August 15, 2003.
[139] Novell Technical Information Document, TID2966741, August 15, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Olivier Muller[140]	Unix	OMail webmail 0.97.3, 0.98.3	A vulnerability exists in the 'checklogin()' function due to insufficient filtering of user-supplied input in the $domainname, $username, and $password variables, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://prdownloads.sourceforge.net/omail/omail-webmail-0.98.5.tar.gz	OMail Webmail Remote Command Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
OpenSLP[141]	Unix	OpenSLP 1.0.0-1.0.11	A vulnerability exists because the 'slpd.all_init' file uses the '/tmp/route.check' temporary file in an unsafe manner, which could let a malicious user obtain elevated privileges.	Upgrades available at: ftp://atualizacoes.conectiva.com.br/9/RPMS//	OpenSLP Insecure Temporary File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Oracle Corporation[142]	Multiple	Oracle9i Enterprise Edition 9.2.0.1, Personal Edition 9.2.0.1, Standard Edition 9.2.0.1	Multiple buffer overflow vulnerabilities exist in the Oracle 9i XML Database (XDB) due to boundary errors, which could let a remote malicious user execute arbitrary code.	Patch available at: http://metalink.oracle.com/	Multiple Oracle XDB FTP / HTTP Services Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Exploits have been published.
Oracle Corporation[143]	Windows NT 4.0/2000, XP, OpenVMS, Unix	Oracle9i Client Edition 9.0.1, 9.2.0.1, 9.2.0.2, Oracle9i Enterprise Edition 9.0.1, 9.2.0.1, 9.2.0.2, Oracle9i Personal Edition 9.0.1, 9.2.0.1, 9.2.0.2, Oracle9i Standard Edition 9.0, 9.0.1-9.0.1.4 9.0.2, 9.2.0.1, 9.2.0.2	Several buffer overflow vulnerabilities exist in the XML database functionality, which could let a remote malicious user cause a Denial of Service.	Workaround and upgrade information available at: http://otn.oracle.com/deploy/security/pdf/2003Alert58.pdf	Oracle XML Database Remote Buffer Overflow	Low	Bug discussed in newsgroups and websites.

[140] Bugtraq, August 21, 2003.
[141] Conectiva Linux Security Announcement, CLA-2003:723, August 18, 2003.
[142] SecurityFocus, August 8, 2003.
[143] Oracle Security Alert 58, August 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP[144]	MacOS X 10.x, Unix	PHP 4.0-4.0.7, 4.1.1, 4.1.2, 4.2.0-4.2.3, 4.3- 4.3.2	A vulnerability exists in the 'dlopen()' function when PHP is used in conjunction with the Apache web server, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP DLOpen Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
php WebSite Develop-ment Team [145]	Windows, Unix	phpWebsite 0.7.3, 0.8.2, 0.8.3, 0.9.3	Multiple vulnerabilities exist in the calendar script when the date parameters are altered, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHP Website Calendar Module	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
php WebSite Develop-ment Team [146]	Windows, Unix	phpWebsite 0.7.3, 0.8.2, 0.8.3, 0.9.3	Several Cross-Site Scripting vulnerabilities exist in the Calendar, PageMaster, Search, and Fatcat modules, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP Website Multiple Module Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHPOut-sourcing [147]	Windows, Unix	Zorum 3.0-3.4	A Cross-Site Scripting vulnerability exists in the 'index.php' script due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Zorum Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHPOut-sourcing [148]	Windows, Unix	Zorum 3.4	A path disclosure vulnerability exists when a malformed URL request using the 'method' parameter (or other parameters) is submitted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Zorum Path Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
phpSecure Site[149]	Multiple	phpSecure Site .4, .5	A vulnerability exists due to an input validation error when handling user input used in database queries, which could let a malicious user obtain sensitive information.	Upgrade available at: ftp://oss.wired-networks.net/phpsecuresite/phpsecuresite-0.1.0.tar.bz2	PHPSecureSite SQL Injection	Medium	Bug discussed in newsgroups and websites.
Poly-spaston Limited [150]	Unix	C-Cart 1.0	An information disclosure vulnerability exists when a malformed HTTP GET request is submitted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	C-Cart Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[144] SecurityFocus, August 13, 2003.
[145] Secunia Security Advisory, August 13, 2003.
[146] Secunia Security Advisory, August 13, 2003.
[147] Securiteam, August 13, 2003.
[148] Zone-h Security Team Advisory, ZH2003-22SA, August 10, 2003
[149] Secunia Security Advisory, August 19, 2003.
[150] Zone-h Security Team Advisory, ZH2003-16SA, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PostNuke Development Team[151]	Windows, Unix	PostNuke 0.7, 0.62-0.64, 0.70-0.72, 0.703, 0.72, PostNuke Phoenix 0.721-0.723	A Cross-Site Scripting vulnerability exists in the 'ttitle' variable in the 'Downloads' and 'Web_Links' modules due to insufficient filtering of HTML from user-supplied input, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PostNuke Downloads / Web_Links Modules Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Real Networks [152]	Windows 95/98/ME/ NT 4.0/2000, XP	RealOne Desktop Manager, RealOne Enterprise Desktop 6.0.11.774, RealOne Player 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0, RealOne Player Gold for Windows 6.0.10 .505	A vulnerability exists due to an unspecified error in the handling of SMIL files, which could let a remote malicious user execute arbitrary code.	Updates available at: http://www.service.real.com/help/faq/security/securityupdate_august2003.html	RealOne Player SMIL File Script Execution	**High**	Bug discussed in newsgroups and websites.
RedHat[153]	Unix	up2date-3.0.7-1.i386.rpm, 3.1.23-1.i386.rpm, gnome-3.0.7-1.i386.rpm, gnome-3.1.23-1.i386.rpm	A vulnerability exists in the up2date tool due to insufficient validation of GPG signatures on rpm packages downloaded from the Red Hat Network, which could let up2date trust an unsigned packages from Red Hat Network.	Update available at: ftp://updates.redhat.com/	Red Hat Linux Up2Date GPG Signature Validation CVE Name: CAN-2003-0546	Medium	Bug discussed in newsgroups and websites.
Russell Marks[154] ***Debian issues advisory*** [155]	**Unix**	**zblast 1.2**	**A buffer overflow vulnerability exists in the 'ZBLAST_NAME,' 'USER,' and 'LOGNAME' variables when data is copied, which could let a malicious user execute arbitrary code.**	***Debian:*** **http://security.debian.org/pool/updates/main/z/zblast/**	**Zblast Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[151] SecurityTracker Alert ID, 1007439, August 8, 2003.
[152] RealNetworks Security Advisory, August 19, 2003.
[153] Red Hat Security Advisory, RHSA-2003:255-01, August 8, 2003.
[154] Bugtraq, June 5, 2003.
[155] Debian Security Advisory, DSA 369-1, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sandsprite .com[156]	Windows	Web ChatServer	An input validation vulnerability exists which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Web ChatServer Arbitrary Code Execution	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
SGI[157]	Unix	IRIX 6.5-6.5.16, 6.5.17 m-6.5.19 m, 6.5.17 f-6.5.19 f	A remote Denial of Service vulnerability exists in the 'nsfd' daemon due to an error in the XDR decoding routines.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/	IRIX NFSD XDR Decoding Remote Denial of Service CVE Name: CAN-2003-0576	Low	Bug discussed in newsgroups and websites.
SGI[158]	Unix	IRIX 6.5-6.5.16, 6.5.17 m - 6.5.21 m, 6.5.17 f - 6.5.21 f	A vulnerability exists due to an error in the 'libcpr' library for the checkpoint/restart (cpr) system, which could let a malicious user corrupt files.	Patches available at: ftp://patches.sgi.com/support/free/security/patches/ http://www.sgi.com/support/security/	SGI IRIX Checkpoint/ Restart libcpr File Corruption CVE Name: CAN-2003-0679	Medium	Bug discussed in newsgroups and websites.
Skunkweb [159]	Unix	Skunkweb 3.3, 3.4 b1-b3	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists because the HTTP 404 error page does not filter HTML code from user-supplied input, which could let a remote malicious user execute arbitrary code; and a Directory Traversal vulnerability exists when a specially crafted URL is submitted, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://sourceforge.net/projects/skunkweb/	Skunkweb Cross-Site Scripting & Directory Traversal	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the Cross-Site Scripting vulnerability. Directory Traversal vulnerability may be exploited via a web browser.
Sun Micro-systems, Inc.[160]	Windows NT 4.0/2000, Unix	iPlanet Directory Server 5.0, 5.1, SP1&SP2; Sun ONE Directory Server 5.1, SP1&SP2, 5.0, SP1&SP2,	Several vulnerabilities exist: a Directory Traversal vulnerability exists in the 'ViewLog' function due to insufficient checking, which could let a remote malicious user obtain sensitive information; and a vulnerability exists because the default installation does not require a password, which could let a remote malicious user obtain access.	Patches available at: **SunOne:** http://docs.sun.com/source/816-6703-10/index.html **iPlanet:** http://docs.sun.com/db/doc/816-6403-10	Sun One / IPlanet Administration Server Directory Traversal & Insufficient Authentication	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[156] Exploitlabs Advisory, EXPL-A-2003-019, August 9, 2003.
[157] SGI Security Advisory, 20030801-01-P, August 13, 2003.
[158] SGI Security Advisory, 20030802-01-P, August 14, 2003.
[159] SecurityTracker Alert ID, 1007489, August 13, 2003.
[160] EDS Information Assurance Group, August 8, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Micro-systems, Inc.[161]	Windows NT 4.0/2000	ONE Web Server 6.0, SP3-SP5	A local/remote Denial of Service vulnerability exists on Windows platforms.	Upgrade available at: http://wwws.sun.com/software/download/products/3f186391.html	Sun One/IPlanet Web Server Windows Denial of Service	Low	Bug discussed in newsgroups and websites.
Sustain-able Softworks [162]	MacOS X	IPNet MonitorX, IPNet SentryX	A vulnerability exists in the 'RunTCPDump' and 'RunTCPFlow' tools due to insufficient authentication procedures, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.sustworks.com/site/downloads.	IPNetSentryX / IPNet MonitorX Helper Tools	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Symantec [163] ***Work-around available [164]***	**Windows 98/ME/NT 2.0/2000, XP**	**Norton AntiVirus 2002, 2003**	**A vulnerability exists due to an error in the 'DeviceIoControl()' function, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code.**	***Workaround:*** ***The vendor has recommended that, because local access is required to exploit this vulnerability, the guest account should be deactivated. Only trusted users should be given interactive access until a patch has been released.***	**Norton AntiVirus 'DeviceIo Control()' Function**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
Univer-sity of Minne-sota[165] ***This software is no longer main-tained[166]***	**Unix**	**gopherd 1.12, 2.0.3, 2.0.4, 2.3, 2.3.1, 3.0.0-3.0.5**	**Two vulnerabilities exist: a buffer overflow vulnerability exists in the 'GopherFile()' function, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'GSisText()' function, which could let a remote malicious user execute arbitrary code.**	***All users of gopherd are advised to immediately upgrade to PyGopherds as UMN gohperd has been removed from distribution and is no longer supported.*** **http://quux.org/devel/gopher/pygopherd** ***It is important to note that all versions of gopherd currently deployed now have known security holes.***	**GopherD Buffer Overflows**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**

[161] Sun(sm) Alert Notification, 56180, August 13, 2003.
[162] @stake, Inc. Security Advisory, a080703-1, August 7, 2003.
[163] Securiteam, August 4, 2003.
[164] SecurityFocus, August 9, 2003.
[165] Bugtraq, July 12, 2003.
[166] Bugtraq, August 18, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Valve Software [167] ***Another exploit script published*** [168]	**Windows 98/NT 4.0**	**Half-Life 1.1 .0.8, 1.1.0.9, 1.1.1.0**	**A buffer overflow vulnerability exists in the client connection routine due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**Half-Life Client Connection Routine Remote Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.** ***Another exploit script has been published.***
VMware Inc.[169]	Unix	VMware Work-station For Linux File Deletion	A vulnerability exists because symlinks can be manipulated, which could let a remote malicious user delete arbitrary files.	Upgrade available at: http://www.vmware.com/vmwarestore/newstore/download.jsp?ProductCode=WKST4-LX-ESD	VMware Workstation For Linux File Deletion	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Wedgetail Commun-ications[170]	Windows, Unix	JCSI SSO suite 1.1	An access validation vulnerability exists because patterns in an XML files used to specify standard access control rules for J2EE web applications are incorrectly matched, which could let a remote malicious user obtain unauthorized access.	**Workaround:** The vendor has recommended that, as a viable workaround, customers ensure that URI paths in the policy XML file match the deployed context-root in all web applications that are protected with JCSI SSO.	JSCI SSO Pattern Matching Access Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Xoops[171]	Windows, Unix	Xoops 1.0 RC3.0.5, RC3, RC1, 1.3.5-1.3.10	A Cross-Site Scripting vulnerability exists in 'BBCode' due to insufficient sanitization of user-supplied BBCode tags, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www.xoops.org//general/download.php	Xoops BBCode Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

[167] Securiteam, July 31, 2003.
[168] SecurityFocus, August 12, 2003.
[169] Secunia Security Advisor, August 8, 2003.
[170] Wedgetail Communications Security Advisory, WSA-20030729-1-0, August 6, 2003.
[171] Bugtraq, August 13, 2003.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between August 7 and August 20, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 31 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 20, 2003	**ftpcrash.pl**	**Perl script that exploits the FTPServer Remote Denial of Service vulnerability.**
August 16, 2003	DOS.c	Script that exploits the Netris Client-Side Buffer Overflow vulnerability.
August 16, 2003	xnetris.c	Script that exploits the Netris Client-Side Buffer Overflow vulnerability.
August 15, 2003	nfm-shatterdame.zip	DameWare Mini Remote Control Server version 3.71.0.0 and below remote exploit that takes advantage of a shatter style attack.
August 14, 2003	dameware-shatter.cpp	Exploit for the Mini Remote Control Server System Access vulnerability.
August 13, 2003	**fm-php-deface.c**	**Script that exploits the PHP DLOpen Information Disclosure vulnerability.**
August 13, 2003	**fm-php-memdump.c**	**Script that exploits the PHP DLOpen Information Disclosure vulnerability.**
August 13, 2003	**phrack61.tar.gz**	**Phrack Magazine Issue 61 - In this issue: Advanced Doug Lea's malloc exploits, Hijacking Linux Page Fault Handler, The Cerberus ELF interface, Polymorphic Shellcode Engine, Infecting Loadable Kernel Modules, Building IA32 Unicode-Proof Shellcodes, Fun with the Spanning Tree Protocol, Hacking da Linux Kernel Network Stack, Kernel Rootkit Experiences, Phrack World News, Loopback, Linenoise, Toolz Armory, Phrack Prophile on DiGiT.**
August 13, 2003	URLScan_enum.tar.gz	Exploit for the Microsoft URLScan / RSA Security SecurID Configuration Enumeration vulnerability.
August 12, 2003	**ibmdb2.pl**	**Perl script that exploits the DB2 'db2job' Arbitrary File Overwrite vulnerability.**
August 12, 2003	lukemftp.pl	Perl script that exploits the FreeBSD realpath() Off-By-One Buffer Overflow vulnerability.
August 12, 2003	multimap.pl	A multithreaded wrapper for nmap designed to run a number of concurrent nmap scans and speed up the scan of large networks.
August 11, 2003	0x82-WOOooouHappy_new.c	Remote root exploit for the Wuftpd Off-by-one vulnerability.
August 11, 2003	firedoor-0.2.tar.gz	Firedoor forwards any TCP connection behind a firewall using techniques similar to reverse Telneting.
August 11, 2003	**kaht2.zip**	**Exploit for the Windows DCOM RPC Buffer Overflow vulnerability.**

Date of Script (Reverse Chronological Order)	Script name	Script Description
August 11, 2003	**m00-HL-portbind.c**	**Script that exploits the Half-Life Client Connection Routine Remote Buffer Overflow vulnerability.**
August 11, 2003	priv8atari800.pl	Perl script that exploits the Atari800 Emulator Buffer Overflow vulnerabilities.
August 11, 2003	**rsvp.c**	**Script that exploits the Windows 2000 RSVP Server Authority Hijacking vulnerability.**
August 10, 2003	airsnarf-0.2.tar.gz	Airsnarf is a simple, rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hotspots.
August 10, 2003	airsnarf-0.2-Zaurus.tar.gz	A Zaurus PDA version of Airsnarf, the rogue wireless access point setup utility designed to demonstrate how a rogue AP can steal usernames and passwords from public wireless hotspots.
August 10, 2003	amap-4.2.tar.gz	Application Mapper is a next-generation scanning tool that allows you to identify the applications that are running on a specific port.
August 10, 2003	CiscoCasumEst.tgz	Exploit for IOS 2GB HTTP GET Buffer Overflow vulnerability.
August 10, 2003	exitwound.tgz	A ptrace shared library redirection backdoor that is based on the technique described in Phrack 59-8. It attempts to redirect certain string handling routines commonly used in Internet services to trapdoored functions which yield a connect back shell on a specifically constructed passphrase.
August 10, 2003	**grenzgaenger-alpha.tar.gz**	**Grenzgaenger is a SOCKS-like hacker tool for tunneling nmap, netcat and exploits transparently through systems into protected networks**
August 10, 2003	iosniff.tgz	Exploit for the IOS UDP Echo Service Information Disclosure vulnerability.
August 10, 2003	**meteordos.pl**	**Perl script that exploits the Meteor FTP Server USER Remote Denial of Service vulnerability.**
August 10, 2003	redirector.cpp	A high performance C++ class that is useful for getting around firewalls and redirecting TCP traffic.
August 8, 2003	IglooExloit.c	Script that exploits the IglooFTP Pro 3.8 vulnerability.
August 8, 2003	xpcd-ex.c	Exploit for the XPCD Home Environment Variable Buffer Overflow vulnerability.
August 7, 2003	postfix.pl	Perl script that exploits the Postfix Malformed E-mail Envelope Address Remote Denial of Service vulnerability.
August 7, 2003	postfixdos.c	Perl script that exploits the Postfix Malformed E-mail Envelope Address Remote Denial of Service vulnerability.

Trends

- **A new worm that exploits the same security weakness as the Blaster worm (also known as "lovsan" or "msblast") has been released on the Internet. This new worm, dubbed "nachi," "welchia," or "msblast.d" does not infect systems that have been updated to counter the Blaster worm in accordance with Microsoft's instructions http://www.microsoft.com/security/incident/blast.asp. This new worm will re-infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself. For more information see "W32/Nachi-A" in the Virus Section and Department of Homeland Security advisory located at: http://www.nipc.gov/warnings/advisories/2003/Advisory8182003.htm**

- **The CERT/CC has received reports of an new variant of the Sobig worm, 'W32/Sobig.F.' Like its' predecessors, Sobig.F attempts to replicate itself by sending out infected e-mail. In addition, it can download and execute arbitrary code on the target machine, which potentially permits the worm to compromise confidential information, or set up and run other services, such as open mail relays. For more information, see "W32/Sobig-F" in the Virus Section and CERT® Incident Note IN-2003-03 located at: http://www.cert.org/incident_notes/IN-2003-03.html**
- **The DHS/Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued a second update to the security advisory on Microsoft's DCOM RPC Buffer Overflow vulnerability. Malicious code dubbed "MSBLAST," "LOVSAN," or "BLASTER" began circulating on the Internet on August 11th. (Additional information regarding this worm can be found in the "Virus" section.) This worm takes advantage of the vulnerability discussed in Microsoft's advisory located at: http://www.microsoft.com/technet/security/bulletin/MS03-026.asp and contains code that will target Microsoft's update servers on August 16th. This additional attack could cause significant Internet-wide disruptions. It is also possible that other worms based on this vulnerability will be released over the next few days as "copy cat" attacks. Also numerous exploits and Trojans have been reported in the wild that exploit this vulnerability. Please ensure that you have applied the Microsoft patch for this vulnerability.**
- **Online vandals are using a program to compromise Windows servers and remotely control them through Internet relay chat (IRC) networks. Several programs, including one that exploits a recent vulnerability in computers running Windows, have been cobbled together to create a remote attack tool. The tool takes commands from a malicious user through the IRC networks and can scan for and compromise computers vulnerable to the recently discovered flaw in Windows**
- **The CERT/CC has received reports of systems being compromised by two recently discovered vulnerabilities in the Microsoft Remote Procedure Call (RPC) service. Additionally, the CERT/CC has received reports of widespread scanning for systems with open Microsoft RPC ports (135, 139, 445). For more information, see "Exploitation of Microsoft RPC Vulnerabilities" located at: http://www.cert.org/current/.**
- **The Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) National Cyber Security Division (NCSD) has issued an advisory in consultation with the Microsoft Corporation to heighten awareness of potential Internet disruptions resulting from the possible spread of malicious software exploiting a vulnerability in popular Microsoft Windows operating systems. DHS expects that exploits are being developed for malicious use. For more information see DHS/IAIP Advisory located: http://www.nipc.gov/warnings/advisories/2003/Potential72403.htm. Additional information on the Microsoft vulnerability may also be found at: http://microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp.**
- **Recent reports to the CERT/CC have highlighted two chronic problems:**
  - **The speed at which viruses are spreading is increasing. This echoes the trend toward faster propagation rates seen in the past few years in self-propagating malicious code (i.e., worms). A similar trend from weeks to hours has emerged in the virus (i.e., non-self-propagating malicious code) arena.**
  - In a number of the reports, users who were compromised may have been under the incorrect impression that merely having antivirus software installed was enough to protect them from all malicious code attacks. This is simply a mistaken assumption, and users must always exercise caution when handling e-mail attachments or other code or data from untrustworthy sources. For more information see, CERT® Incident Note IN-2003-01, located at: http://www.cert.org/incident_notes/IN-2003-01.html.

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT.Randren (Batch File Worm): BAT.Randren is a virus written as a batch file. This batch file will only work on Microsoft Windows XP, as it relies on a variable that is not set by default on any other Microsoft OS.

BAT.Rous.worm (Alias: I-Worm.Rous.A) (Batch File Worm): This batch script sends itself via IRC. It attempts to delete files belonging to various antivirus programs and also to overwrite .bat and .con files found in the %Windir% folder.

O97M_TORAJA3.C (Aliases: O97M/Toraja.C, X97M/Toraja) (Office 97 Macro Virus): This multi-platform macro virus works on Microsoft Office 97 and Office 2000 applications, specifically Word and Excel. It uses Visual Basic for Applications (VBA) codes to infect Word documents, Excel sheets ands templates. It also has the ability to infect across these documents. The virus deletes 11250 characters from the start of the infected document and all data found in Excel sheet cell A1 to J17. It also disables macro virus protection on Word and Excel 97.

VBS.DDV.B (Visual Basic Script Worm): This Visual Basic Script worm attempts to spread to all the contacts in the Microsoft Outlook address book. The worm is similar to VBS.DDV, but makes additional destructive modifications to the registry.

W32.Bacterra.Worm (Alias: Worm.P2P.Bacterra.a) (Win32 Worm): This worm attempts to spread via the eDonkey2000 file-sharing program. The worm is written in the Visual Basic programming language.

W32.Blaster.B.Worm (Aliases: WORM_MSBLAST.B, Win32.Poza.C, W32/Lovsan.worm.c, W32/Lovsan.worm, Worm.Win32.Lovesan, W32/Blaster-B, W32.Blaster.Worm, Win32.Poza, Lovsan.B) (Win32 Worm): This is a variant of the W32.Blaster.Worm that exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026), using TCP port 135. The worm targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems. This worm attempts to download the penis32.exe file to the %WinDir%\System32 folder, and then execute it. This worm does not have any mass-mailing functionality.

W32.Blaster.C.Worm (Aliases: W32/Blaster-B, W32/Lovsan.worm.b, Win32.Poza.B) (Win32 Worm, Lovsan.C) (Win32 Worm): This worm exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. It targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to the aforementioned exploit (if not properly patched), the worm is not coded to replicate to those systems. This worm attempts to download the Teekids.exe file to the %WinDir%\System32 folder, and then execute it. It does not have any mass-mailing functionality. This worm may have been distributed in a package which also contained a backdoor Trojan. The worm also attempts to perform a Denial of Service (DoS) on the Microsoft Windows Update Web server (www.windowsupdate.com). This is an attempt to prevent you from applying a patch on your computer against the DCOM RPC vulnerability.

W32/Blaster-D (Aliases: W32/Lovsan.worm.d, Exploit-DcomRpc Trojan, WORM_MSBLAST.E, Lovsan.D, W32/Msblast.D) (Win32 Worm): This worm spreads in the same way as W32/Blaster-A. However, the Blaster-D variant is packed differently, uses the filename (and process name) mspatch.exe instead of msblast.exe, and adds the registry entry

- HKLM\Software\Microsoft\Windows\CurrentVersion\Runon\Norton Antivirus

Microsoft issued a patch for the vulnerability exploited by this worm on July 16, 2003.

W32.Bugsoft (Alias: Bloodhound.W32.VBWORM) (Win32 Worm): This intended worm, written in Microsoft Visual Basic, attempts to send itself to all the contacts in the Microsoft Outlook Address Book. When the worm is executed, it displays a message box.

W32.Dinkdink.Worm (Win32 Worm): This worm exploits the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. It targets only Windows 2000 and Windows XP machines. While Windows NT and Windows 2003 Server machines are vulnerable to this exploit if it is not properly patched, the worm is not coded to replicate to those systems. The worm uses a two-step procedure to spread itself, using a fixed server from which to download itself.

W32/Dumaru-A (Alias: PE_DUMARU.A, Win32.Dumaru, W32/Dumaru@MM, W32.Dumaru@mm, WORM_DUMARU.A, Dumaru, I-Worm.Dumaru) (Win32 Worm): This virus spreads using e-mail and infects other executable using NTFS Alternate Data Stream. The virus arrives in an e-mail message with the following characteristics:

- Sender: "Microsoft" <security@microsoft.com>
- Subject line: Use this patch immediately !
- Attached file: patch.exe

When the attachment is run, the worm copies itself into the Windows folder as dllreg.exe and into the Windows system folder as load32.exe and vxdmgr32.exe. It drops and runs <Windows>\windrv.exe, a backdoor Trojan. The virus creates the registry value load32 of the following registry key so that the virus file <Windows system>\load32.exe is run on Windows startup:

- \HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

W32/Gaobot.worm.y (Alias: Backdoor.Agobot.3, WORM_AGOBOT.P, W32.HLLW.Gaobot.AA) (Win32 Worm): This worm attempts to use the following Microsoft vulnerabilities to spread: MS03-001 (RPC Locator) and MS03-026 (DCOM RPC). The worm then copies itself to the WINDOWS SYSTEM directory and references itself in the registry so that it will be loaded again at startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Config Loader" = svchosl.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "Config Loader" = svchosl.exe

The worm needs MSVCP60.DLL to run - this is a standard MS Visual C DLL but if it is not present the worm would not be able to execute.

W32.HLLW.Antinny (Aliases: W32/Antinny.worm) (Win32 Worm): This that spreads on the Winny file-sharing network. When the worm is executed, it displays a fake error message in Japanese. The worm is written in Microsoft Visual C++.

W32.HLLW.Aritim (Win32 Worm): This worm with process-injection capabilities attempts to spread itself through file-sharing networks. The existence of the file Aritima.exe is an indication of a possible infection.

W32.HLLW.Cult.H@mm (Win32 Worm): This mass-mailing worm uses its own SMTP engine to send itself to randomly generated recipient names from a variety of domains. The e-mail message has the following characteristics:

- Subject: I Love You ^_^ I sent you a beautiful Love Card
- Attachment: BlueMountaineCard.pif

The worm also has IRC Trojan functionality that allows the Trojan's creator to control the infected computer by using Internet Relay Chat (IRC). This threat is compressed with ASPack.

W32.HLLW.Habrack (Aliases: W32/Habrack.worm!p2p, W32/Habrack.bat, W32/Habrack.vbs) (Win 32 Worm): This worm attempts to spread through file-sharing networks. The worm also has backdoor functionalities that allow its creator to control a compromised system. When the worm is executed, it displays fake messages. This threat is written in the Microsoft Visual Basic programming language.

W32.HLLW.Lemur (Win32 Worm): This worm spreads through the KaZaA file-sharing network. It is written in the Microsoft Visual Basic programming language.

W32.HLLW.Moega (Alias: Backdoor.Sdbot.gen, W32/Sdbot.worm.gen, W32/Donk-C) (Win32 Worm): This worm with backdoor capabilities attempts to spread through the local network. The worm attempts to open ports 139 and 445, as well as steal sensitive information. When the worm is executed, it will appear as an icon. The worm is packed with UPX.

W32.HLLW.Shydy.B (Win32 Worm): This worm attempts to spread through the KaZaA and iMesh file-sharing networks. The worm is written in Microsoft Visual Basic, and is packed with UPX. The Visual Basic run-time libraries must be installed for the worm to execute.

W32.HLLW.Tofaced (Win32 Worm): This worm attempts to spread through file-sharing networks. The worm also continually accesses the floppy drive.

W32.HLLW.Yodo (Win32 Worm): This worm spreads through the KaZaA file-sharing network. It copies itself as C:\Windows\System32\Updater.exe. The worm is written in the Microsoft Visual Basic programming language.

W32.Kuskus.Worm (Win32 Worm): This worm, written in Visual Basic, spreads through file-sharing networks.

W32.Mant.Worm (Aliases: Worm.P2P.Milcan, W32/Milcan.worm!p2p) (Win32 Worm): This worm spreads through the KaZaA and Morpheus file-sharing networks. It may cause system instability due to bugs in its code.

W32.Miniman@mm (Alias: I-Worm.Miniman) (Win32 Worm): This mass-mailing worm sends itself to all the contacts in the Microsoft Outlook address book.. The worm is written in the Microsoft Visual Basic (VB) language.

W32/Nachi-A (Aliases: W32/Welchia.worm10240, W32/Nachi.worm, WORM_MSBLAST.D, Lovsan.D, W32.Welchia.Worm, Welchi, Nachi, Welchia, Win32.Nachi.A, Sachi, Worm.Win32.Welchia)(Win32 Worm): This worm spreads using the RPC DCOM vulnerability in a similar fashion to the W32/Blaster-A worm. It attempts to spread using a buffer overflow exploit for ntdll.dll library in several versions of Microsoft Windows. Once the system is infected, W32/Nachi-A attempts to download and run security patches from the Microsoft's update websites. If the security patch is successfully downloaded the worm attempts to restart the system. When the main service routine is launched, it checks for the existence of the process name and the filename of W32/Blaster-A. If the process exists the worm attempts to terminate it and to remove the file. The worm removes itself from the system on January 1, 2004.

W32.Nuffy.A (Aliases: W32.Nuf.A, Worm.Win32.Nuf) (Win32 Worm): This worm propagates via open network shares. It does not contain a damaging payload.

W32/Pandem-B (Aliases: W32.Pandem.B.Worm, W32/Squirm@mm, (Win32 Worm): This worm spreads via e-mail by copying itself to the shared folders of various peer-to-peer networks and displays the messages "Security Patch 329390 Patching system... Wait" and "Security Patch 329390 Patched. Thanks for using Microsoft Windows." W32/Pandem-B then drops the file ZLIB.DLL into the Windows system folder and copies itself to the Windows folder as CPUMGR.EXE. The worm creates the following registry entry to run itself on system restart:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\CPU Manager = <Windows>\CPUMGR.EXE

It also drops PHOTO.ZIP (a zipped copy of the worm called COOL.SCR), CPUMGR.DLL (an encoded copy of the worm) and PDMN.SMT (a text file containing the SMTP domain) in the Windows folder. E-mails sent by the worm have the following characteristics:

- From: support@microsoft.com
- Subject line: "Microsoft Security Bulletin"
- Attached file: PATCH.ZIP (containing PATCH_329390.EXE).

W32.Panol@mm (Win32 Worm): This mass-mailing worm uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: The easy, automatic way to keep your PC virus-free
- Attachment: Virus_scanner.exe

This threat is written in the Microsoft Visual Basic programming language and is compressed with UPX

W32.Randex.F (Aliases: Backdor.IRCBot.gen, W32/Sluter.worm) (Win32 Worm): This network-aware worm copies itself as the following files:

- \Admin$\system32\NETFD32.EXE \c$\winnt\system32\NETFD32.EXE

The worm will receive instructions from an IRC channel on a specific IRC server. One such command will trigger the aforementioned spreading.

W32.Randex.G (Aliases: W32/Randex.worm.c, Backdoor.SdBot.gen) (Win32 Worm): This network-aware worm that will copy itself as the following files:

- \Admin$\system32\NETFD32.EXE \c$\winnt\system32\NETFD32.EXE

The worm will receive instructions from an IRC channel on a specific IRC server. One such command will trigger the aforementioned spreading.

W32.Randex.H (Win32 Worm): This variant of W32.Randex.F connects to an IRC channel on a specific IRC and waits for instructions from its creator. The worm is packed with Krypton v0.5.

W32/Sobig-F (Aliases: I-Worm.Sobig.f, Win32.Sobig.F, W32/Sobig.F-mm, W32/Sobig.f@MM, W32.Sobig.F@mm, WORM_SOBIG.F, Sobig.F) (Win32 Worm): The worm sends itself, using its own SMTP engine, as an attachment to e-mail addresses collected from various files on the victim's computer. When it distributes itself via e-mail it forges the sender's e-mail address, making it difficult to know who is truly infected. The e-mail includes one of the following attachments: movie0045.pif wicked_scr.scr; application.pif document_9446.pif; details.pif; your_details.pif; thank_you.pif; document_all.pif; your_document.pif. It also attempts to spread by copying itself to Windows network shares and uses the Network Time Protocol to one of several servers in order to determine the current date and time. The worm stops working on September 10 2003 or later.

W32.Sowsat.B@mm (Alias: I-Worm.Sowsat.f) (Win32 Worm): This mass-mailing worm spreads by using its own SMTP engine. The e-mail will have variable subjects and variable attachment names. The attachment should have a .exe file extension. An e-mail claiming to be from Symantec was spammed to a large number of individuals in an attempt to get users to download and execute this worm. This worm is written in Borland Delphi and is packed with UPX.

W32.Sowsat.C@mm (Win32 Worm): This is a variant of W32.Sowsat@mm, a mass-mailing worm that spreads by using its own SMTP engine and spreads through IRC. The e-mail has a variable subject line and attachment name. The attachment should have a .exe file extension. The worm is written in Borland Delphi and is packed with UPX.

W32/Spybot.worm.lz (TrojanDropper.Win32.Small.bd, W32.Randex.E, WORM_RPCSDBOT.A, Win32:RPCexploit, IRC-BBot, W32/RpcSpybot-A, Exploit-DcomRPC, Backdoor.Sdbot.au, TrojanDropper.Win32.Small.bd, Sdbot.RPC.A) (Win32 Worm): This worm exploits the MS03-026 vulnerability. It works in a similar fashion to W32/Lovsan.worm in that it creates a remote shell on TCP Port 4444 and tells the compromised target system to download (TFTP) and execute the worm from the host system. This threat differs in that it is also an IRC bot (the source code for IRC-Sdbot was used). When run, the worm creates two files in the %WinDir%\System32 directory:

- C:\WINNT\system32\winlogin.exe (24,064 bytes)
- C:\WINNT\system32\yuetyutr.dll (43,520 bytes)

Several registry run keys are created to load the worm at system startup (note regedit will simply display the value as winlogin.exe):

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Runonce "winlogon" = winlogin.exe linuzguy unchained rage 1.1 MIRC CHAIN SCRIPT tateravo asdasd#$@#$#@ASFDASASFASFASASASDASASFASDFASDASSDA SOFTWARE\
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run "NDplDeamon" = winlogin.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run "winlogon" = winlogin.exe linuzguy unchained rage 1.1 MIRC CHAIN SCRIPT tateravo asdasd#$@#$#@ASFDASASFASFASASASDASASFASDFASDASSDA SOFTWARE\
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ Winlogon "Shell" = explorer.exe winlogin.exe

WORM_FRANRIV.A (Internet Worm): This proof-of-concept program demonstrates how a game construction kit, such as the popular Game Maker, can be used maliciously. The program supports registry and file manipulation and even the execution of any program. Due to bugs in its code, however, the worm program may not run properly. It propagates via the popular peer-to-peer file sharing network KaZaA and requires that the folder C:\Windows exists before it executes. As a result, it may not run on Windows NT and 2000, since the folder is not found on typical installations of these platforms. Note, however, that this worm can execute smoothly on Windows 95, 98, ME, NT, 2000, and XP machines that have the folder C:\Windows.

WORM_SLANPER.A (Aliases: win32.HLLW.Slanper, W32/Slanper.worm.gen, W32/Slanper) (Win32 Worm): This network-aware worm spreads to random remote machines through SMB shares via port 445. It has a backdoor component that listens on the following ports to receive remote commands: 3330, 3331, and 3332. This UPX-compressed worm is written and compiled in Visual C++ and runs on Windows NT, 2000, and XP.

WORM_THRAX.A (Internet Worm): To propagate, this multi-component worm targets Windows 2000, NT and XP systems with weak administrator passwords. The malware's main executable file is a fake or crafted mIRC program that controls its malicious behavior through its scripts. As an efficient measure, it uses legitimate third party tools for such malicious purposes as hiding its malicious activities and running programs on remote target systems. It runs under Windows 95, 98, ME but fails to propagate because of the path and other features used that are not available on the said windows versions.

WORM_WUKILL.A (Alias: Win32/VBWorm2@mm) (Internet Worm): This nondestructive worm mass-mails copies of itself to all the addresses listed in the Windows Address Book (WAB). It sends out an e-mail with the following details:

- Subject: &ltnone>
- Attachment: MShelp.EXE

However, it only works successfully when run under the Windows folder.

Worm/Darby (Alias: W32/Darby.worm; W32.Darby.Worm; Worm.P2P.VB.ai; W32/P2P.Zade) (P2P Worm): This Internet worm spreads through e-mail by using file-sharing programs like KaZaA and Edonkey2000. If executed, the worm copies itself in the following locations:

- C:\windows\%system%\<7 random digits>.<exe, pif or com extension>
- C:\windows\%system%\<7 random digits>.<exe, pif or com extension>
- C:\windows\%system%\<7 random digits>.<exe, pif or com extension>
- C:\windows\%tmpdir%\Template.xls.scr
- C:\windows\%tmpdir%\Bt1.b
- C:\windows\%tmpdir%\Bt2.b
- C:\windows\%tmpdir%\Bt3.b

The worm will copy itself to the following directories: "C:\Program Files\Kazaa\My Shared Folder\" and "C:\Program Files\eDonkey2000\incoming\" with a variety of filenames. So that it gets run each time a user restart their computer the following registry keys get added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\Run "MicroLoad"="C:\\WINDOWS\\SYSTEM\\<7 random digits>.com"
- HKEY_LOCAL_MACHINE\Software\GEDZAC LABS\W32.Bardiel

The following key gets modified:

- HKEY_CURRENT_USER\Software\Microsoft\WindowsNT\CurrentVersion\Policies\System

Worm/Urick.D (Alias: I-Worm.Urick.d) (Internet Worm): This Internet worm spreads through the use of the file sharing program KaZaA. If executed, the worm copies itself in the following locations:

- C:\msdos.exe
- C:\My Documents\Sex Rated.doc.EXE

So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices @="C:\\MSDOS.EXE"

Additionally, the following registry key also gets added in under to spread through KaZaA:

HKEY_CURRENT_USER\Software\Kazaa\LocalContent
"dir0"="012345:C:\\"
HKEY_CURRENT_USER\Software\Kazaa\LocalContent
"dir1"="012345:C:\\My Documents"

Worm/Urick.E (Alias: I-Worm.Urick.e) (Internet Worm): This is a variation of Worm/Urick.D, an Internet worm that spreads through the use of the file sharing program KaZaA. Variant E arrives as "black_worm.exe."

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
Adware-SubSearch.dr	dr	CyberNotes-2003-14
AIM-Canbot	N/A	CyberNotes-2003-07
AprilNice	N/A	CyberNotes-2003-08
Backdoor.Acidoor	N/A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Amitis.B	B	CyberNotes-2003-11
Backdoor.AntiLam.20.K	K	CyberNotes-2003-10
Backdoor.Apdoor	N/A	CyberNotes-2003-12
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Assasin.F	F	CyberNotes-2003-09
Backdoor.Badcodor	N/A	CyberNotes-2003-12
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.Cli	Cli	CyberNotes-2003-10
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.dr	dr	CyberNotes-2003-16
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Beasty.G	G	CyberNotes-2003-16
Backdoor.Bigfoot	N/A	CyberNotes-2003-09
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CamKing	N/A	CyberNotes-2003-10
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Cmjspy	N/A	CyberNotes-2003-10
Backdoor.Cmjspy.B	B	CyberNotes-2003-14
Backdoor.CNK.A	A	CyberNotes-2003-10
Backdoor.CNK.A.Cli	Cli	CyberNotes-2003-10
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Death.Cli	Cli	CyberNotes-2003-10
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.Cli	Cli	CyberNotes-2003-10
Backdoor.Delf.F	F	CyberNotes-2003-07
Backdoor.Drator	N/A	CyberNotes-2003-01
Backdoor.Dsklite	N/A	CyberNotes-2003-14
Backdoor.Dsklite.cli	cli	CyberNotes-2003-14
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.EggDrop	N/A	CyberNotes-2003-08
Backdoor.Fatroj	N/A	CyberNotes-2003-10
Backdoor.Fatroj.Cli	Cli	CyberNotes-2003-10
Backdoor.Fluxay	N/A	CyberNotes-2003-07
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	C	CyberNotes-2003-07
Backdoor.FTP_Ana.D	D	CyberNotes-2003-08
Backdoor.Fxdoor	N/A	CyberNotes-2003-10
Backdoor.Fxdoor.Cli	Cli	CyberNotes-2003-10
Backdoor.Fxsvc	N/A	CyberNotes-2003-16
Backdoor.Graybird	N/A	CyberNotes-2003-07

Trojan	Version	CyberNotes Issue #
Backdoor.Graybird.B	B	CyberNotes-2003-08
Backdoor.Graybird.C	C	CyberNotes-2003-08
Backdoor.Graybird.D	D	CyberNotes-2003-14
Backdoor.Grobodor	N/A	CyberNotes-2003-12
Backdoor.Guzu.B	B	CyberNotes-2003-14
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hale	N/A	CyberNotes-2003-16
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Aladinz.C	C	CyberNotes-2003-14
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Comiz	N/A	CyberNotes-2003-11
Backdoor.IRC.Flood.F	F	CyberNotes-2003-16
Backdoor.IRC.Lampsy	N/A	CyberNotes-2003-10
Backdoor.IRC.PSK	PSK	CyberNotes-2003-16
Backdoor.IRC.Ratsou	N/A	CyberNotes-2003-10
Backdoor.IRC.Ratsou.B	B	CyberNotes-2003-11
Backdoor.IRC.Ratsou.C	C	CyberNotes-2003-11
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Kaitex.D	D	CyberNotes-2003-09
Backdoor.Kalasbot	N/A	CyberNotes-2003-09
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kodalo	N/A	CyberNotes-2003-14
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.Lala.B	B	CyberNotes-2003-16
Backdoor.Lala.C	C	CyberNotes-2003-16
Backdoor.Lanfilt.B	B	CyberNotes-2003-14
Backdoor.Lastras	**N/A**	**Current Issue**
Backdoor.LeGuardien.B	B	CyberNotes-2003-10
Backdoor.Litmus.203.c	c	CyberNotes-2003-09
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Lorac	**N/A**	**Current Issue**
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MindControl	N/A	CyberNotes-2003-14
Backdoor.Monator	N/A	CyberNotes-2003-08
Backdoor.Mots	N/A	CyberNotes-2003-11
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.Netdevil.15	15	CyberNotes-2003-15
Backdoor.NetDevil.B	B	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Nibu	N/A	CyberNotes-2003-16
Backdoor.Nickser	N?A	CyberNotes-2003-14
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	N/A	CyberNotes-2003-07
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	12.b	CyberNotes-2003-07
Backdoor.OptixPro.13	13	CyberNotes-2003-09
Backdoor.Peers	N/A	CyberNotes-2003-10
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.Pointex	N/A	CyberNotes-2003-09
Backdoor.Pointex.B	B	CyberNotes-2003-09
Backdoor.Private	N/A	CyberNotes-2003-11
Backdoor.Prorat	N/A	CyberNotes-2003-13
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Ratega	N/A	CyberNotes-2003-09
Backdoor.Recerv	N/A	CyberNotes-2003-09
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Roxy	N/A	CyberNotes-2003-16
Backdoor.Rsbot	N/A	CyberNotes-2003-07
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	F	CyberNotes-2003-07
Backdoor.Sdbot.G	G	CyberNotes-2003-08
Backdoor.Sdbot.H	H	CyberNotes-2003-09
Backdoor.Sdbot.L	L	CyberNotes-2003-11
Backdoor.Sdbot.M	M	CyberNotes-2003-13
Backdoor.Sdbot.P	**P**	**Current Issue**
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Simali	N/A	CyberNotes-2003-09
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Slao	N/A	CyberNotes-2003-11
Backdoor.Snami	N/A	CyberNotes-2003-10
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.Softshell	N/A	CyberNotes-2003-10
Backdoor.Stealer	N/A	CyberNotes-2003-14
Backdoor.SubSari.15	15	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.Sumtax	N/A	CyberNotes-2003-16
Backdoor.Syskbot	N/A	CyberNotes-2003-08
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	N/A	CyberNotes-2003-07
Backdoor.Trynoma	N/A	CyberNotes-2003-08
Backdoor.Turkojan	N/A	CyberNotes-2003-07
Backdoor.Udps.10	1	CyberNotes-2003-03
Backdoor.UKS	N/A	CyberNotes-2003-11
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.Uzbet	N/A	CyberNotes-2003-15
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Winet	N/A	CyberNotes-2003-11
Backdoor.WinJank	N/A	CyberNotes-2003-15
Backdoor.Winker	N/A	CyberNotes-2003-15
Backdoor.WinShell.50	N/A	CyberNotes-2003-16
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.XTS	N/A	CyberNotes-2003-08
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdemon.126	126	CyberNotes-2003-10
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zombam	N/A	CyberNotes-2003-08
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	ASD	CyberNotes-2003-07
BackDoor-ASL	ASL	CyberNotes-2003-07
BackDoor-ASW	ASW	CyberNotes-2003-08
BackDoor-ATG	ATG	CyberNotes-2003-09
BackDoor-AUP	N/A	CyberNotes-2003-11
BackDoor-AVF	AVF	CyberNotes-2003-12
BackDoor-AVH	AVH	CyberNotes-2003-12
BackDoor-AVO	AVO	CyberNotes-2003-12
BackDoor-AXC	AXC	CyberNotes-2003-14
BackDoor-AXQ	AXQ	CyberNotes-2003-15
Backdoor-AXR	AXR	CyberNotes-2003-16
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02

Trojan	Version	CyberNotes Issue #
BDS/CheckESP	N/A	CyberNotes-2003-12
BDS/Ciadoor.10	10	CyberNotes-2003-07
BDS/Evilbot.A	A	CyberNotes-2003-09
BDS/Evolut	N/A	CyberNotes-2003-03
BDS/GrayBird.G	**G**	**Current Issue**
BDS/PowerSpider.A	A	CyberNotes-2003-11
BKDR_LITH.103.A	**A**	**Current Issue**
CoolFool	**N/A**	**Current Issue**
Daysun	N/A	CyberNotes-2003-06
DDoS-Stinkbot	N/A	CyberNotes-2003-08
DoS-iFrameNet	N/A	CyberNotes-2003-04
Download.Trojan.B	B	CyberNotes-2003-13
Downloader.BO.B	B	CyberNotes-2003-10
Downloader.BO.B.dr	B.dr	CyberNotes-2003-10
Downloader.Dluca	**N/A**	**Current Issue**
Downloader.Mimail	N/A	CyberNotes-2003-16
Downloader-BN.b	BN.b	CyberNotes-2003-13
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	BW.c	CyberNotes-2003-07
Downloader-CY	CY	CyberNotes-2003-16
Downloader-DM	DM	CyberNotes-2003-16
Downloader-DN.b	**DN.b**	**Current Issue**
ELF_TYPOT.A	A	CyberNotes-2003-13
ELF_TYPOT.B	B	CyberNotes-2003-13
Exploit-IISInjector	N/A	CyberNotes-2003-03
Gpix	N/A	CyberNotes-2003-08
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC/Flood.bu	bu	CyberNotes-2003-08
IRC/Flood.cd	cd	CyberNotes-2003-11
IRC/Flood.cm	cm	CyberNotes-2003-13
IRC/Fyle	N/A	CyberNotes-2003-16
IRC-BBot	N/A	CyberNotes-2003-16
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
IRC-Vup	N/A	CyberNotes-2003-09
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Fortnight.c@M	c	CyberNotes-2003-11

Trojan	Version	CyberNotes Issue #
JS/Seeker-C	C	CyberNotes-2003-04
JS/StartPage.dr	dr	CyberNotes-2003-11
JS_WEBLOG.A	A	CyberNotes-2003-05
Keylogger.Cone.Trojan	N/A	CyberNotes-2003-14
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Keylf	**N/A**	**Current Issue**
Keylog-Kjie	N/A	CyberNotes-2003-12
Keylog-Perfect.dr	dr	CyberNotes-2003-09
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Keylog-Yeehah	N/A	CyberNotes-2003-12
Linux/DDoS-Ferlect	**N/A**	**Current Issue**
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
Lockme	N/A	CyberNotes-2003-15
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-AH	AH	CyberNotes-2003-08
ProcKill-AJ	AJ	CyberNotes-2003-13
ProcKill-Z	N/A	CyberNotes-2003-03
Proxy-Guzu	N/A	CyberNotes-2003-08
Proxy-Migmaf	N/A	CyberNotes-2003-14
PWS-Aileen	N/A	CyberNotes-2003-04
PWS-Sincom.dr	**dr**	**Current Issue**
PWSteal.ABCHlp	N/A	CyberNotes-2003-12
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Bancos	N/A	CyberNotes-2003-15
PWSteal.Bancos.B	B	CyberNotes-2003-16
PWSteal.Hukle	N/A	CyberNotes-2003-08
PWSteal.Kipper	N/A	CyberNotes-2003-10
PWSteal.Lemir.105	105	CyberNotes-2003-10
PWSteal.Lemir.C	**C**	**Current Issue**
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Rimd.B	B	CyberNotes-2003-10
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWSteal.Snatch	N/A	CyberNotes-2003-10
PWSteal.Sysrater	N/A	CyberNotes-2003-12
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-Train	**N/A**	**Current Issue**
PWS-Truebf	N/A	CyberNotes-2003-13
PWS-Watsn	N/A	CyberNotes-2003-10
PWS-Wexd	N/A	CyberNotes-2003-14
PWS-WMPatch	N/A	CyberNotes-2003-07
PWS-Yipper	N/A	CyberNotes-2003-10
QDel359	359	CyberNotes-2003-01
QDel373	373	CyberNotes-2003-06
Qdel374	374	CyberNotes-2003-06
Qdel375	375	CyberNotes-2003-06

Trojan	Version	CyberNotes Issue #
Qdel376	376	CyberNotes-2003-07
QDel378	378	CyberNotes-2003-08
QDel379	369	CyberNotes-2003-09
QDel390	390	CyberNotes-2003-13
QDel391	391	CyberNotes-2003-13
QDel392	392	CyberNotes-2003-13
QDial11	1	CyberNotes-2003-14
QDial6	6	CyberNotes-2003-11
Renamer.c	N/A	CyberNotes-2003-03
Reom.Trojan	N/A	CyberNotes-2003-08
StartPage-G	G	CyberNotes-2003-06
Startpage-N	N	CyberNotes-2003-13
Stealther	N/A	CyberNotes-2003-16
Stoplete	N/A	CyberNotes-2003-06
Swizzor	N/A	CyberNotes-2003-07
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	21	CyberNotes-2003-07
Tr/Delf.r	r	CyberNotes-2003-16
Tr/DelWinbootdir	N/A	CyberNotes-2003-07
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
TR/Gaslide.C	**C**	**Current Issue**
Tr/SpBit.A	A	CyberNotes-2003-04
Tr/VB.t	T	CyberNotes-2003-11
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Ataka-E	E	CyberNotes-2003-15
Troj/Autoroot-A	A	CyberNotes-2003-16
Troj/Bdoor-RQ	**RQ**	**Current Issue**
Troj/Dloader-BO	BO	CyberNotes-2003-02
Troj/DownLdr-DI	DI	CyberNotes-2003-15
Troj/Golon-A	A	CyberNotes-2003-15
Troj/Hacline-B	B	CyberNotes-2003-13
Troj/IRCBot-C	C	CyberNotes-2003-11
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Migmaf-A	A	CyberNotes-2003-15
Troj/Mystri-A	A	CyberNotes-2003-13
Troj/PcGhost-A	A	CyberNotes-2003-13
Troj/Peido-B	B	CyberNotes-2003-10
Troj/QQPass-A	A	CyberNotes-2003-16
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Sandesa-A	A	CyberNotes-2003-14
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
Troj/Webber-A	A	CyberNotes-2003-15
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Trojan.Ailati	N/A	CyberNotes-2003-15
Trojan.Analogx	**N/A**	**Current Issue**
Trojan.AprilFool	N/A	CyberNotes-2003-08
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Guapeton	N/A	CyberNotes-2003-08
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.Kaht	N/A	CyberNotes-2003-10
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Lear	N/A	CyberNotes-2003-10
Trojan.Mumuboy	N/A	CyberNotes-2003-13
Trojan.Myet	N/A	CyberNotes-2003-12
Trojan.OptixKiller	N/A	CyberNotes-2003-16
Trojan.Poetas	N/A	CyberNotes-2003-14
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.PopSpy	N/A	CyberNotes-2003-11
Trojan.Progent	N/A	CyberNotes-2003-16
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Sarka	N/A	CyberNotes-2003-14
Trojan.Sidea	N/A	CyberNotes-2003-12
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Trojan.Visages	N/A	CyberNotes-2003-15
Trojan.Windelete	N/A	CyberNotes-2003-14
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	D.b	CyberNotes-2003-07
VBS.ExitWin	N/A	CyberNotes-2003-12
VBS.Flipe	**N/A**	**Current Issue**
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS.Zizarn	N/A	CyberNotes-2003-09
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Adclicker.C.Trojan	C	CyberNotes-2003-09
W32.Bambo	N/A	CyberNotes-2003-14

Trojan	Version	CyberNotes Issue #
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Laorenshen.Trojan	N/A	CyberNotes-2003-14
W32.Noops.Trojan	N/A	CyberNotes-2003-09
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Spybot.dr	dr	CyberNotes-2003-15
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Trabajo	N/A	CyberNotes-2003-14
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Woodcot	N/A	CyberNotes-2003-16
Xin	N/A	CyberNotes-2003-03

Backdoor.Lastras: This Trojan gives its creator unauthorized access to your computer and is written in Microsoft Visual Basic.

Backdoor.Lorac: This backdoor Trojan allows remote control of an infected system, via HTTP. It has been distributed as an e-mail attachment named Message.zip and an HTML file, which contains the Trojan, exists inside the zip file. The Trojan takes advantage of a vulnerability described in Microsoft Security Bulletin MS03-14, which allows for the execution of a MIME-encoded program inside an HTML file.

Backdoor.Sdbot.P (Aliases: Backdoor.SdBot.gen, W32/Sdbot.worm.gen): This Backdoor Trojan Horse is a variant of Backdoor.Sdbot that allows the Trojan's creator to use Internet Relay Chat (IRC) to gain access to an infected computer.

BDS/GrayBird.G (Alias: Backdoor.Graybird): This Trojan would potentially allow a malicious user remote access to your computer. If executed, the backdoor remains memory resident and adds the following file to the \windows\%system% directory, "SP00LSV.EXE." It will also modify the "win.ini" file. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "SP00LSV"="C:\\WINDOWS\\SYSTEM\\SP00LSV.EXE"
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices "SP00LSV"="C:\\WINDOWS\\SYSTEM\\SP00LSV.EXE"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "SP00LSV"="C:\\WINDOWS\\SYSTEM\\SP00LSV.EXE"

It does not spread itself over e-mail but arrived in user's inbox with the following e-mail characteristics, most likely directly distributed by its creator in an attempt to get users to install the backdoor.

- From: webmaster@microsoft.com
- Subject: updated
- Attachment: 03-26updated.exe

BKDR_LITH.103.A (Aliases: Backdoor.Lithium.103, Backdoor:Win32/Lithium.1_03): This Trojan enables a remote malicious user to access and manipulate a target machine by utilizing its server and client components. The server component installs on the target machine, and once active, opens a port and waits for client connection. Upon establishing port connection, the client program which is controlled by a remote malicious user, may then issue commands that leaves the target system's security adversely compromised.

CoolFool: The file is 252,416 bytes in length and may arrive attached to an e-mail message. The Trojan also contains an embedded DLL file with a length of 73,728 bytes that is installed by the Trojan. When run, the Trojan copies itself to the %SYSTEM% folder on the local system using a randomly generated name (i.e. EOI3QFRP.EXE, O3FZMZPJ.EXE) and creates the registry key

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\SystemManager=FILENAME.EXE

Downloader.Dluca (Alias: TrojanDownloader.W32.Dluca.e): This downloader Trojan Horse sends information about your computer to a specific Web site and creates a shortcut on your Windows desktop.

Downloader-DN.b: Written in MSVC, this downloader Trojan bears strong similarities to a previous version, Downloader-DN. It has been spammed to many users via e-mail messages with the following characteristics:

- Subject: Re[2]: photos
- Attachment: PHOTO1.JPG.SRC

The attachment extension is not directly executable on typical machines. Presumably the latter extension was intended to be .SCR. When run, it displays a fake error message prior to downloading and executing a file from a remote server (URL hardcoded within the downloader Trojan). The remote file is downloaded to the Windows System directory using a filename also hardcoded in the Trojan:

- C:\WINDOWS\SYSTEM\TMP2334.EXE

Keylog-Keylf: This Key logger Trojan logs any key pressed to a file. The file can be mailed out via SMTP mail. It comes in a self-extracted archive. When run, the following three files are created:

- %SysDir%mswin.exe
- %SysDir%keylogf.dll
- %SysDir%GpSysHookDLL.dll

The following registry key is created in order to load the Trojan at Windows startup:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "MSWin" = %SysDir%mswin.exe

Linux/DDoS-Ferlect (Aliases: DDoS.Linux.Reflect, ELF_FERLECT.A): The malicious ELF type binary file has a filesize of 15947 bytes. The drdos v1.0 is a demonstration of distributed reflection Denial of Service attacks. By default it's using port 80 but another port may be specified

PWSteal.Lemir.C (Aliases: Trojan.PWS.Legendmir.s, PWS-LegMir): This Trojan Horse attempts to steal the password for the "Legend of Mir 2" online game and send it to the Trojan's author. The Trojan is written in Microsoft Visual C++ and is UPX-packed.

PWS-Sincom.dr: This is the dropper component of the Trojan PWS-Sincom. Different variants of this dropper may exist, so filenames and registry keys might be different. Upon execution, the password-stealer is dropped into network drives with the following filenames:

- Explorer.exe (hidden)
- autorun.inf

The autorun.inf file enables the Trojan to be run automatically if it was written to a CD-ROM drive.

PWS-Train: This password stealing Trojan is designed to e-mail the encoded local passwords to the Trojan author. When the dropper is executed it drops the real password stealer WINDOWS folder as 1.exe and creates a text file in WINDOWS\TEMP as 1.txt. It then add the following registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run "putil"="c:\WINDOWS\1.EXE"

The text file is displayed with the default txt viewer. After that the real password stealer is executed. It contacts the SMTP server at 194.67.23.10 and mails the encoded passwords found on the system.

TR/Gaslide.C (Aliases: Trojan.Win32.Gaslide.c, Gaslide): This Trojan would potentially allow a malicious user backdoor access to your computer. If executed, the Trojan adds the following files to the \windows\temp\ directory, "nload.vxd" and "helpctl.exe." So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "C:\\WINDOWS\\TEMP\\HELPCTL.EXE"="C:\\WINDOWS\\TEMP\\HELPCTL.EXE"

Additionally, the following registry key is added:

- HKEY_LOCAL_MACHINE\Software\CLASSES\exefile\shell\open\command@="\"%1\" %*"@="C:\\WINDOWS\\SYSTEM\\CDRUNXP.EXE \"%1\" %*"

After the creation of the files and registry key entries it will delete the following files from the infected machine:

- C:\windows\notepad.exe
- C:\windows\system\notepad.exe
- C:\windows\notepad32.exe

Troj/Bdoor-RQ: This modified copy of the netcat utility is used to read and write data over network connections. This modified version is coded to listen on a specific port and return a command prompt to a malicious user when they Telnet to that port. The versions of this modified tool listen on ports 99, 1984 and 5000.

Trojan.Analogx: This Trojan is a modified version of the AnalogX proxy server, which installs and configures the proxy server, and then launches it. The Trojan is written in Borland Delphi and is UPX-packed.

VBS.Flipe (Aliases: Trojan.VBS.Flipe.a, VBS/Sillytrojan.A): This Trojan Horse attempts to format hard disk drives and floppy drives.